NEWSLETTER

July 2019

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

VOLUME 3 ISSUE 3

@NCIIPC

NCIIPC Newsletter

July 2019

स्वच्छ भारत

एक कदम स्वच्छता की ओर

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

Collaboration among Government, Industry, Academia and Cybersecurity Researchers is an important facet of working towards achieving success in protection of Critical Information Infrastructure (CII). As part of the multi-stakeholder approach, NCIIPC had initiated the 'Responsible Vulnerability Disclosure Program' (RVDP) to leverage cyber research community to identify the vulnerabilities related to Indian critical assets and report them to NCIIPC. This has been a resounding success.

Considering the overwhelming response, NCIIPC organised a one-day RVDP Convention on 2nd July 2019 at New Delhi. The event focused on acknowledging the contributions of the RVDP researchers' and reaching out to others to join hands in protecting national CII.

We have introduced a 'Guest Article' section from this edition of NCIIPC Newsletter where we invite articles from various experts and NCIIPC stakeholders to share their experience, views and expertise in protecting the CII.

> *We have introduced a 'Guest Article' section from this edition of NCIIPC Newsletter where we invite articles from various experts and NCIIPC stakeholders*

United States has announced a new approach for identification of Critical Infrastructure based on critical functions. This is a paradigm shift from the current sector specific approach. They have also directed their agencies to reduce the time to patch critical vulnerabilities from 30 to 15 days, in view of the exploits being released very rapidly on discovery of new vulnerabilities. The European Union has prepared a protocol to counter cross border cyber-attacks. Cybersecurity officials from 30 countries met at Prague, Czech Republic on 2nd May 2019 to draw a blueprint for security of next generation mobile networks, which is an ongoing global concern.

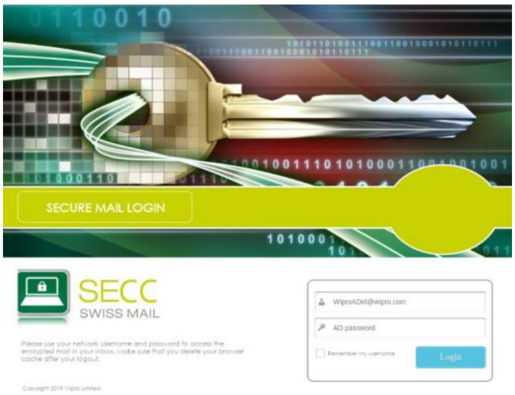
Comments, suggestions and feedback are solicited from the readers to enhance the content of subsequent issues. You may like to write to us at newsletter@nciipc.gov.in

News Snippets - National

Indian IT Firms attacked by an Advanced Phishing Campaign

Source: https://tech.economictimes.indiatimes.com/, https://krebsonsecurity.com/

Indian IT firm Wipro Ltd. confirmed that its IT systems were attacked and it has hired a forensic firm, after cybersecurity website KrebsOnSecurity reported about the attacks. The site reported that it was an intrusion from an assumed state-sponsored attacker for few months. “We detected a potentially abnormal activity in a few employee accounts on our network due to an advanced phishing campaign. Upon learning of the incident, we promptly began an investigation, identified the affected users and took remedial steps to contain and mitigate any potential impact,” Wipro Ltd said in a statement to ET. “We are leveraging our industry-leading cyber security practices and collaborating with our partner ecosystem to collect and monitor advanced threat intelligence for enhancing security posture. We have also retained a well-respected, independent forensic firm to assist us in the investigation. We continue to monitor our enterprise and infrastructure at a heightened level of alertness,” the Wipro statement added. The offenders responsible for launching phishing campaigns that netted dozens of employees and more than 100 computer systems at Wipro also appeared to have targeted a number of other companies. The clues suggested this was the work of a fairly experienced crime group that is focused on perpetrating gift card fraud.



SECURE MAIL LOGIN

SECC
SWISS MAIL

Please use your network username and password to access the encrypted mail in your inbox. Make sure that you delete your browser cache after your logout.

WiproADid@wipro.com

AD password

□ Remember my username

Login

Copyright 2019 Wipro Limited

A screen shot of the Wipro phishing site securemail.wipro.com.internal-message[.]app. Image: urlscan.io

News Snippets - International

Several US Airlines Flights affected due to Aerodata Outage

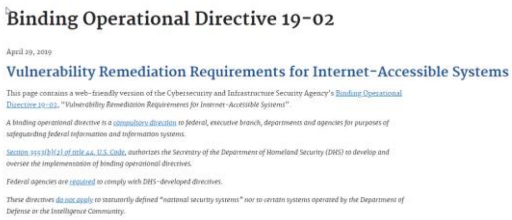
Source: https://www.bleepingcomputer.com/

Several U.S. airlines including Southwest Airlines, American Airlines, Delta Air Lines, United Airlines, Alaska Airlines, and JetBlue experienced issues with their computing systems on 1st April 2019 leading to flight cancellations and delay because of the IT issues faced by the third-party contractor Aerodata's flight planning weight and balance program. Aerodata offers aircraft performance data, weight and balance data, and load planning services to the airline industry. Also, AeroData’s flight deck client-server application is the last application used by pilots before the aircraft entry door is closed prior to take-off. As a result, just five minutes of system downtime can result in hundreds of delayed flights and consequent loss of revenue.

Image Source: https://www.express.co.uk/

Aerodata offers aircraft performance data, weight and balance data, and load planning services to the airline industry.

DHS directs Agencies to Rapidly Remediate Vulnerabilities



Binding Operational Directive 19-02

April 29, 2019

Vulnerability Remediation Requirements for Internet-Accessible Systems

This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 19-02, "Vulnerability Remediation Requirements for Internet-Accessible Systems"

A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems.

Section 3553(b)(2) of title 44, U.S. Code, authorizes the Secretary of the Department of Homeland Security (DHS) to develop and oversee the implementation of binding operational directives.

Federal agencies are required to comply with DHS-developed directives.

These directives do not apply to statutorily defined "national security systems" nor to certain systems operated by the Department of Defense or the Intelligence Community.

Source: https://cyber.dhs.gov, https://federalnewsnetwork.com

The US Department of Homeland Security (DHS) directed federal agencies to rapidly remediate vulnerabilities that otherwise could allow malicious actors to compromise federal networks through exploitable, externally-facing systems. DHS issued a new Binding Operational Directive (BOD) setting the new deadlines for vulnerabilities identified through cyber hygiene scanning. The 2015 requirement to fix critical system vulnerabilities in 30 days is now cut to half, and agencies must fix "high" vulnerabilities in 30 days. Also, BOD starts tracking vulnerabilities from the point of initial detection, rather than the date of first report to agencies. Recent reports from government and industry partners indicate that the average time between discovery and exploitation of vulnerability is decreasing as today's adversaries are more skilled, persistent, and able to exploit known vulnerabilities. DHS wants agencies to inform them of any remediation constraints, what interim steps they are taking to overcome those constraints and estimated completion date to address the cyber problem. DHS says they will hold agencies accountable, in part, through the Federal Cyber Exposure Scorecard.

Recent reports from government and industry partners indicate that the average time between discovery and exploitation of vulnerability is decreasing as today's adversaries are more skilled, persistent, and able to exploit known vulnerabilities.

Baltimore Government hit by another Ransomware Attack

Image Source: Sean Pavone/Getty Images

Source: https://www.fifthdomain.com/, https://www.nextgov.com/

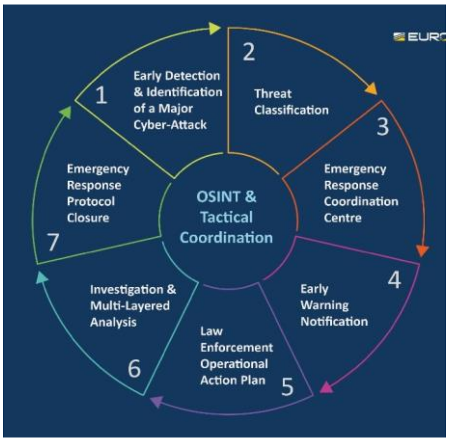
Baltimore's government had to shut down most of its computer servers after its network was hit by a ransomware virus. Hackers reportedly used an NSA tool called EternalBlue to freeze thousands of the Baltimore government's computers. The attack was first reported by Baltimore's Department of Public Works, when the department's official Twitter account announced that its email access was cut off, and it reported phones and other systems were affected soon afterward. In response to this, the city's Office of Information Technology team shut down nearly all of the city's non-emergency systems to prevent the further spread of the attack. It's reported that the city's email and IP-based phones were among the systems affected. Further, Baltimore has no insurance to cover the cost of a cyber-attack. The problems came just over a year since another ransomware attack hit Baltimore's 911 dispatch system, prompting 17-hour shutdown of automated emergency dispatching.

City's Office of Information Technology team shut down nearly all of the city's non-emergency systems to prevent the further spread of the attack.

EU Prepared Protocol to counter Cross Border Cyber Attacks

Source: https://www.europol.europa.eu

In order to prepare for major cross-border cyber-attacks, an EU Law Enforcement Emergency Response Protocol has been adopted by the Council of the European Union.


1
Early Detection & Identification of a Major Cyber-Attack
2
Threat Classification
3
Emergency Response Coordination Centre
4
Early Warning Notification
5
Law Enforcement Operational Action Plan
6
Investigation & Multi-Layered Analysis
7
Emergency Response Protocol Closure
OSINT & Tactical Coordination

The Protocol gives a central role to Europol's European Cybercrime Centre (EC3) and is part of the EU Blueprint for Coordinated Response to large-scale cross-border Cybersecurity incidents and crises. It serves as a tool to support the EU law enforcement authorities in providing immediate response to major cross-border cyber-attacks through rapid assessment, the secure and timely sharing of critical information and effective coordination of the international aspects of their investigations. The protocol is a multi-stakeholder process and entails total of seven possible core stages from the early detection and the threat classification to the closure of the Emergency Response Protocol. As the EU Agency for law enforcement cooperation, Europol is mandated to support the Member States' endeavours to effectively detect, investigate, disrupt and deter large-scale cyber incidents of a suspected criminal nature.

Microsoft takes control of 99 Websites used for Cyberattacks

Source: https://blogs.microsoft.com

Microsoft's Digital Crimes Unit disrupted cyberattacks from a threat group called Phosphorus – also known as APT 35, Charming Kitten, and Ajax Security Team. Microsoft used court order to take control of 99 websites that were being used to conduct cyberattacks and redirected its traffic from infected devices to its Digital Crime Unit's sinkhole. Phosphorus' activity is usually designed to gain access to the computer systems of businesses and government agencies and steal sensitive information. Phosphorus typically attempts to compromise the personal accounts of individuals through a technique known as spear-phishing, using social engineering to entice someone to click on a link, sometimes sent through fake social media accounts that appear to belong to friendly contacts. The link contains malicious software that enables Phosphorus to access computer systems. Phosphorus also uses a technique whereby it sends people an email that makes it seem as if there's a security risk to their accounts, prompting them to enter their credentials into a web form that enables the group to capture their passwords and gain access to their systems. Both attack methods employ the use of websites that incorporate the names of well-known brands, like Microsoft, to appear authentic.

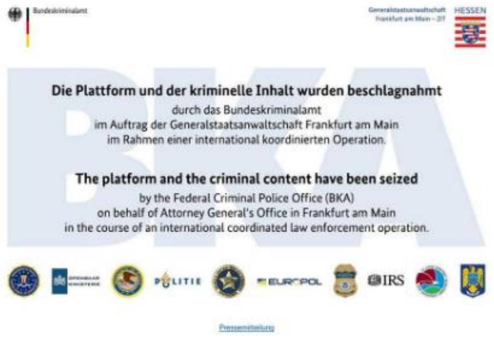
> *Attack methods employ the use of websites that incorporate the names of well-known brands, like Microsoft, to appear authentic.*

Dark Web Marketplaces - Wall Street and Silkkitie taken down

Source: https://www.europol.europa.eu

In a simultaneous global operation, two dark web marketplaces - the Wall Street Market and the Silkkitie were taken down.

This operation was supported by Europol. The online marketplace Wall Street market was the world's second largest dark web market, enabling the trade of drugs, stolen data, fake documents and malicious software etc. The illegal platform was exclusively accessible via the Tor network in the Darknet. For payment, the users of the online marketplace used the crypto currencies Bitcoin and Monero. Another marketplace, the Silkkitie (known as the Valhalla Marketplace) has been operating on the Tor network since 2013. For several years, narcotics and other illicit goods have been sold via this marketplace. Europol has established a dedicated Dark Web Team to work together with EU partners and law enforcement across the globe to reduce the size of this underground illegal economy. The team aims to enhance joint technical and investigative actions, organise training and capacity-building initiatives, together with prevention and awareness-raising campaigns – a 360° strategy against criminality on the dark web.



Bundeskriminalamt

Generalstaatsanwaltschaft
Frankfurt am Main – ZIT

HESSEN

Die Plattform und der kriminelle Inhalt wurden beschlagnahmt
durch das Bundeskriminalamt
im Auftrag der Generalstaatsanwaltschaft Frankfurt am Main
im Rahmen einer international koordinierten Operation.

The platform and the criminal content have been seized
by the Federal Criminal Police Office (BKA)
on behalf of Attorney General's Office in Frankfurt am Main
in the course of an international coordinated law enforcement operation.

Pressemitteilung

Trends

The Five Most Dangerous New Attack Techniques

Source: https://www.eweek.com/

Attackers are constantly changing tactics as they aim to gain an upper hand on defenders and un-suspecting victims. Following are the most dangerous new attack techniques as discussed by SANS researchers in RSA conference 2019.

DNS Manipulation: Attackers are making use of stolen credentials in order to log into domain registry systems and change information. To help limit the risk of DNS manipulation, organizations must use multi-factor authentication and deploy DNSsec to improve the authenticity of DNS records.

Domain Fronting: Domain Fronting is a technique used by attackers, to obscure where the attacker is located, where the command and control is coming from and where the bad guy is exfiltrating trading data to. To help limit the risk of domain fronting, enterprises should not blindly trust traffic going to and from their cloud providers.

Targeted Individual Attacks: The hackers are able to collect a user's information via a number of different mechanisms, which enables the hackers to get access to user accounts. To limit the risk, users must review their cloud settings to see what is publicly available and take steps to limit the availability of personal information.

> *The hackers are able to get access to a user's information via a number of different mechanisms, which enables the hackers to get access to user accounts.*

DNS Information Leakage: With DNS information an attacker can gain insight into where traffic is headed. That same capability however is useful for defenders to understand how attack traffic is coming in and where it is headed.

The challenge of DNS information leakage can be solved by encrypting the DNS traffic, with DNS over HTTPS, though this approach also makes it more difficult for defenders to spot evil stuff on the network.

Hardware Flaws in BMC: Baseboard Management Controller (BMC) is an integral part of many modern IT systems providing a way to monitor and manage firmware and hardware. These systems can sometimes have vulnerabilities that attackers can potentially exploit. To reduce the risk of hardware management system vulnerabilities users, remove un-needed management utilities and monitor access to the management consoles that are needed.

DARPA is building an Open Source, Secure Voting System

Source: https://www.vice.com/, https://www.fifthdomain.com

The United States Defence Advanced Research Projects Agency (DARPA) is working on to build a secure voting system that will be impermeable to hacking. The first-of-its-kind system will be designed by a firm called Galois, with experience in designing secure and verifiable systems. The system will use fully open source voting software and will be built on secure open source hardware, made from secure designs and techniques developed as part of a special program at DARPA. The voting system will also be designed to create fully verifiable and transparent results so that voters don't have to blindly trust that the machines and election officials delivered correct results. DARPA will design two basic voting machine types. The first will be a ballot-marking device that uses a touch-screen for voters to make their selections. That system won't tabulate votes. Instead it will print out a paper ballot marked with the voter's choices, so voters can review them before depositing them into an optical-scan machine that tabulates the votes. The optical-scan system will print a receipt with a cryptographic representation of the voter's choices. After the election, the cryptographic values for all ballots will be published on a web site, where voters can verify that their ballot and votes are among them.

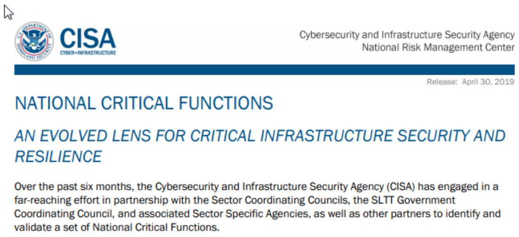
Image Source: https://blogs.microsoft.com

> *After the election, the cryptographic values for all ballots will be published on a web site, where voters can verify that their ballot and votes are among them.*

CISA marks list of Critical Functions making shift from CI Sectors

Source: https://www.dhs.gov/

The United States Cybersecurity and Infrastructure Security Agency (CISA) engaged in a far-reaching effort to identify and validate a set of National Critical Functions. National Critical Functions are defined as the functions of government and the private sector so vital that their disruption, corruption, or dysfunction would have a debilitating effect on national security, national economic, public health or safety, or any combination thereof.



CISA CYBER+INFRASTRUCTURE

Cybersecurity and Infrastructure Security Agency
National Risk Management Center

Release: April 30, 2019

NATIONAL CRITICAL FUNCTIONS

AN EVOLVED LENS FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Over the past six months, the Cybersecurity and Infrastructure Security Agency (CISA) has engaged in a far-reaching effort in partnership with the Sector Coordinating Councils, the SLTT Government Coordinating Council, and associated Sector Specific Agencies, as well as other partners to identify and validate a set of National Critical Functions.

The National Critical Functions construct provides a risk management approach that focuses on better understanding the functions that an entity enables or to which it contributes, rather than focusing on a static sector-specific or asset world view. This more holistic approach is better at capturing cross-cutting risks and associated dependencies that may have cascading impact within and across sectors. It also allows for a new way to view criticality, which is linked to the specific parts of an entity that contribute to critical functions. By viewing risk through a functional lens, it can ultimately add resilience and harden systems across the critical infrastructure ecosystem in a more targeted, prioritized and strategic manner, CISA said in a notification.

It also allows for a new way to view criticality, which is linked to the specific parts of an entity that contribute to critical functions.

Countries draw a Blueprint for safety of 5G Mobile Networks

Source: https://www.fifthdomain.com/

Czech Republic's Prime Minister Andrej Babis holds a speech at The Prague 5G Security Conference in Prague, Czech Republic, May 2, 2019. (Petr David Josek/AP)

Cybersecurity officials from dozens of countries drew up a blueprint to counter threats and ensure the safety of next generation mobile networks that their nations are set to start deploying. Officials hammered out a set of non-binding proposals published at the end of a two-day meeting organized by the Czech government to discuss the security of new 5G networks. Officials called for a cooperative approach to security, saying that they didn't want to target specific countries or companies. The document said "security and risk assessment of vendors and network technologies" should be taken into account, as well as "the overall risk of influence on a supplier by a third country," especially its "model of governance." "Security and risk assessments of vendors and network technologies should take into account rule of law," it said. At the meeting in Prague, the cybersecurity officials came mainly from countries that are strategic allies, including European Union member states, the United States and its Asia-Pacific allies including Australia, Japan and South Korea and Singapore. NATO and European Union officials also participated. However, China and Russia were not present.

Officials called for a cooperative approach to security, saying that they didn't want to target specific countries or companies.

123456 is the most used Password followed by 123456789

Source: https://www.bbc.com/

The United Kingdom's National Cyber Security Centre (NCSC) analysed public databases of breached accounts to see which words, phrases and strings people used. Top of the list was 123456, appearing in more than 23 million passwords. The second-most popular string, 123456789, was not much harder to crack, while others in the top five included "qwerty", "password" and 1111111. The most common name to be used in passwords was Ashley, followed by Michael, Daniel, Jessica and Charlie.

When it comes to Premier League football teams in guessable passwords, Liverpool is the first choice followed by Chelsea. Blink-182 topped the charts of music acts. The NCSC study also quizzed people about their security habits and fears. It found that 42% expected to lose money to online fraud and only 15% said they felt confident that they knew enough to protect themselves online. The NCSC said people should string three random but memorable words together to use as a strong password.

The NCSC said people should string three random but memorable words together to use as a strong password.

Malware Bytes

Project TajMahal: A Highly Sophisticated Spying Framework

Source: https://securelist.com/project-tajmahal/90240/

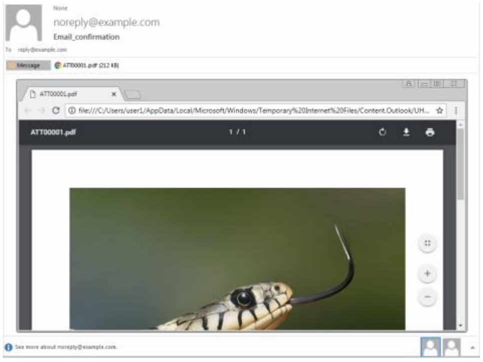
Kaspersky Lab discovered a technically sophisticated spying framework named 'TajMahal' capable of stealing documents from printer queue, backup list of Apple mobile devices, taking screenshots, stealing written CD images, files previously seen on removable devices once they are again available, browser cookies etc. It has been in use for at least since 2013 and the first confirmed samples were seen on August 2014. At first, 'Tokyo' module of TajMahal framework is deployed in victim's machine followed by the 'Yokohama' package which is left in for backup purposes. It consists of up to 80 malicious modules stored in its encrypted Virtual File system. It includes backdoors, loaders, orchestrators, C2 communicators, audio recorders, key loggers, screen and webcam grabbers, documents and cryptography key stealers, and its own file indexer for the victim's machine. If deleted from Frontend file or related registry values, it will reappear after reboot with a new name and start-up type. TajMahal APT sampled is detected as HEUR:Trojan.Multi.Chaperone.gen by Kaspersky Lab. So far Kaspersky have detected a single victim – a diplomatic entity from a country in Central Asia. A likely hypothesis is that there are other victims that haven't been found yet.

So far Kaspersky have detected a single victim – a diplomatic entity from a country in Central Asia. A likely hypothesis is that there are other victims that haven't been found yet.

LightNeuron targeting Government and Diplomatic Entities

Source: https://www.welivesecurity.com/

According to ESET researchers, a sophisticated backdoor, dubbed 'LightNeuron' has been targeting Microsoft Exchange mail servers since at least 2014. This is work of the espionage group Turla, also known as Snake. Three victim organizations such as Brazil, Ministry of Foreign Affairs of Eastern Europe and Regional Diplomatic Organization of Middle East were found during the recent Turla campaign. Its activity aligns with a typical 9-to-5 workday in UTC+3 time zone and corresponds to holidays around the Eastern Orthodox Christmas.

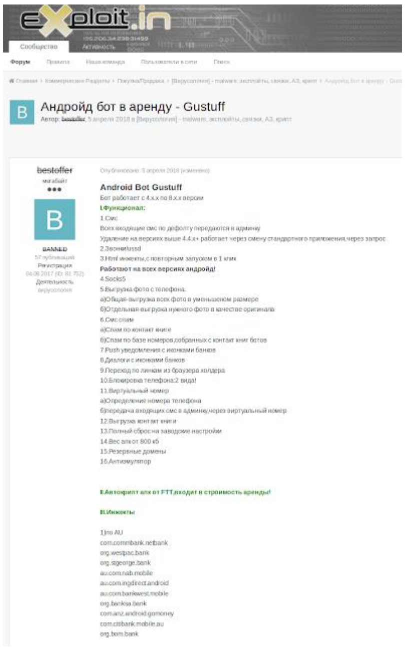


None
noreply@example.com
Email_confirmation
To reply@example.com
Message ATT00001.pdf (212 KB)
ATT00001.pdf
file:///C:/Users/user1/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/UH...
ATT00001.pdf 1 / 1
See more about noreply@example.com.

An email generated by LightNeuron to send command output

Its operators mainly focus on high-profile targets such as governments and diplomatic entities in Europe, Central Asia and the Middle East.

LightNeuron uses a persistence technique never before seen called Transport agent which in the mail server operates at same level of trust as security products such as spam filter. It is able to read and modify any email going through the mail server, compose and send new emails and block any email. LightNeuron uses steganography to hide its command inside a PDF document or a JPG image embedded within an email. Its operators mainly focus on high-profile targets such as governments and diplomatic entities in Europe, Central Asia and the Middle East. They are known for having breached major organizations such as the US Department of Defence in 2008 and the Swiss defence company RUAG in 2014. More recently, several European countries including France and the Czech Republic went public to denounce Turla's attacks against their governments. LightNeuron is hard to detect at the network level because it does not use standard HTTP(S) communications.



eXploit.in
Сообщество
Активность
Форум
Правила
Наша команда
Пользователи в сети
Поиск
Главная > Коммерческие Разделы > Покупка/Продажа > [Вирусология] - malware, эксплойты, связки, АЗ, крипт > Андройд бот в аренду - Gus

Андройд бот в аренду - Gustuff

Автор: bestoffer, 5 апреля 2018 в [Вирусология] - malware, эксплойты, связки, АЗ, крипт

bestoffer
мегабайт
BANNED
57 публикаций
Регистрация
04.08.2017 (ID: 81 752)
Деятельность
вирусология

Опубликовано: 5 апреля 2018 (изменено)

Android Bot Gustuff

Бот работает с 4.х.х по 8.х.х версии

I.Функционал:

1.Смс

Всех входящие смс по дефолту передаются в админку

Удаление на версиях выше 4.4.х+ работает через смену стандартного приложения,через запрос

2.Звонки/ussd

3.Html инжекты,с повторным запуском в 1 клик

Работают на всех версиях андройд!

4.Socks5

5.Выгрузка фото с телефона.

а)Общая-выгрузка всех фото в уменьшеном размере

б)Отдельная выгрузка нужного фото в качестве оригинала

6.Смс спам

а)Спам по контакт книге

б)Спам по базе номеров,собранных с контакт книг ботов

7.Push уведомления с иконками банков

8.Диалоги с иконками банков

9.Переход по линкам из браузера холдера

10.Блокировка телефона:2 вида!

11.Виртуальный номер

а)Определение номера телефона

б)передача входящих смс в админку,через виртуальный номер

12.Выгрузка контакт книги

13.Полный сброс на заводские настройки

14.Вес апк от 800 кб

15.Резервные домены

16.Антиэмулятор

II.Автокрипт апк от FTT,входит в стоимость аренды!

III.Инжекты

1)по AU
com.commbank.netbank
org.westpac.bank
org.stgeorge.bank
au.com.nab.mobile
au.com.ingdirect.android
au.com.bankwest.mobile
org.banksa.bank
com.anz.android.gomoney
com.citibank.mobile.au
org.bom.bank

Gustuff malware being advertised in the Exploit.in forum as a botnet for rent

A New Campaign Targeting Australian Financial Institutions

Source: https://blog.talosintelligence.com/

Cisco Talos came across a new Android-based campaign targeting Australian financial institutions. It is known as 'Gustuff' malware. The primary focus of this malware is stealing credentials, users contact list, collecting phone numbers associated names, and files and photos on the device. The information collected can be used to perform more complex social engineering attacks. SMS is the primary infection vector of this malware which further receives instructions from C2 to spread. Usually, this message targets four or five people at a time. The body contains a message and URL. Again, the concept is that new victims are more likely to install the malware if the SMS comes from someone they know. When a victim tries to access the URL in the SMS body, the C2 will check if the mobile device meets the criteria to receive the malware. The same infrastructure has been used to deploy similar campaigns using different versions of the malware. It binds a large number of permissions in its manifest file and also has various protections placed both in the C2 and malware's code. The code is obfuscated and also packed. The malware also checks for Android SafetyNet and prevents detection by checking for emulators to prevent analysis in sandboxes. It also protects itself by checking for existing anti-virus software installed on the mobile phone.

APT40: Suspected Chinese Cyber Espionage Group

Source: https://www.infosecurity-magazine.com/

FireEye researchers have discovered APT40 which is suspected to be a Chinese state-sponsored group supporting China's efforts to improve its navy, and Belt and Road initiative.

APT40 was also previously ascribed to the TEMP.Periscope and TEMP.Jumper groups. The group has targeted naval research institutes to acquire advanced technology to support the development of Chinese naval capabilities. FireEye also claimed that the group uses domains registered in China with logins configured in Mandarin. FireEye claimed with "moderate confidence" that the group is state-sponsored, saying the targets are consistent with China's interests, attacks center around China Standard Time, and C&C domains were registered in China with logins configured in Mandarin. APT40 often weaponised vulnerabilities within days of public disclosure.

FireEye researchers have discovered APT40 which is suspected to be a Chinese state-sponsored group supporting China's efforts to improve its navy, and Belt and Road initiative.

Learning

Colorado created a new Model to deal with Cyberattack

Source: https://statescoop.com/

Colorado Department of Transportation (CDOT) was affected by the Samsam ransomware in February 2018. This incident affected nearly 2,000 computers, servers and network devices. In total, the ransomware infected 1,274 laptops, 427 desktops, 339 servers, 158 databases, 154 software applications and all voice-over-IP phones used by CDOT at 200 locations across the entire state. IT workers struggled to get a complete picture of the affected systems after discovering the state did not maintain an offline version of its network map. Colorado created a new model for state and local governments to deal with this cyberattack. It handled it like a natural disaster. A state-wide emergency was declared by Colorado Government after the initial infection was detected. It created a unified command structure. The first task after this attack was to establish recovery priorities starting with CDOT's financial operations. Other priorities included protecting traffic operations by keeping those systems separated from the infected portion of CDOT's network. In such incident planning priorities were based on consensus. Despite all these up and downs, disaster management approach proved effective. About 80 percent of CDOT's systems were recovered within a month of the initial attack.

It handled it like a natural disaster. A state-wide emergency was declared by Colorado Government after the initial infection was detected.

Cyber Hygiene Automation

Sh. Rahul Bhatnagar, NCIIPC

Automation applied to the cyber-hygiene framework of enterprises information infrastructure can help proactively and reactively against the volatile threat landscape. In vogue, cyberattacks have become heavily programmed.

If enterprises/organizations try to defend against these bombardments manually, the fight becomes man versus machine, with highly unfavourable odds for the organization. For the prevention against these cybernetic attacks, it is essential to retaliate by incorporating automation into cybersecurity efforts. Automation reduces the volume of threats, and allows for faster prevention of old and latest unknown threats. Automation should also be viewed as a tool that can, and should, be used to better predict behaviours and execute protections faster. If implemented appropriately and with the right tools, automation can aide in the prevention of successful cyberattacks. The following are four ways automation should be used:

If enterprises/organizations try to defend against these bombardments manually, the fight becomes man versus machine, with highly unfavourable odds for the organization. For the prevention against these cybernetic attacks, it is essential to retaliate by incorporating automation into cybersecurity efforts.

Count/Correlating Assets/Data: For protecting the organisation's information assets/data from the risks of unauthorised access, disclosure, damage or interruption to IT related services, enterprises must be aware of their assets/data that is connected to and running on network. Enterprise networks are constantly changing as infrastructure is updated and new servers and services are deployed. Enterprises must be aware of all Internet-connected devices. Anything online is a potential attack vector. Good cybersecurity hygiene tracks existing assets and any changes must be noticed.

Configuration: Many attacks occur due to human error in misconfigured servers. The configuration of the system should ensure that only authorised users are allowed to operate. Enterprises should automate configuration, deployment, and compliance with security in mind.

Control: Automation must be done with security in mind. The necessary activities to be carried out for operation and maintenance of systems or services and actions to be taken in the event of failures shall be designed and developed to ensure the Confidentiality, Integrity and Availability of specific applications.

Patch: Automation patching will acquire, test and install multiple patches (code changes) on existing applications and software tools on a computer, thereby enabling systems to stay updated on existing patches and determining which patches are the appropriate ones. This will help enterprises from unauthorised changes to their IT infrastructure.

Cyber Hygiene Automation will help the enterprises, once a threat has been identified. Protection mechanisms need to be created and distributed faster than the attack spreading throughout the enterprise networks, endpoints or cloud.

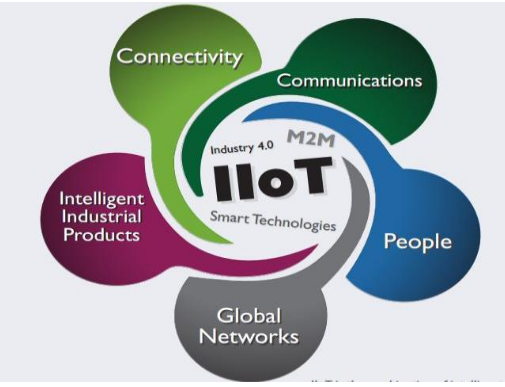
References

[1] https://www.paloaltonetworks.com/cyberpedia/4-ways-cybersecurity-automation-should-be-used

Cyber Security in Industrial Internet of Thing

Sectoral Coordinator (Power and Energy), NCIIPC

The Industrial Internet of Things (IIoT) refers to interconnected sensors, instruments, and other devices networked together with computer industrial applications, including Big Data and Machine Learning. This connectivity allows for data collection, exchange, and analysis, which facilitates improved productivity and efficiency as well as other economic benefits. IIoT goes beyond the normal consumer devices and internetworking of physical devices usually associated with IoT. What makes it distinct is the intersection of Information Technology (IT) and Operational Technology (OT). The convergence of IT and OT provides industries with greater system integration in terms of automation and optimization, as well as better visibility of the supply chain and logistics. Monitoring and control of physical infrastructures in industrial operations, such as in agriculture, healthcare, manufacturing, transportation, and utilities, are made easier through the use of smart sensors and actuators as well as remote access and control.



Challenges in Adopting IIoT: Adoption of IIoT can revolutionize how industries operate, but there is the challenge of having strategies in place to boost digital transformation efforts while maintaining security amid increased connectivity. OT is being integrated into the Internet; organizations are seeing the introduction of more intelligent and automated machines at work, which in turn invites a slew of new challenges that would require understanding of the IIoT's inner workings.

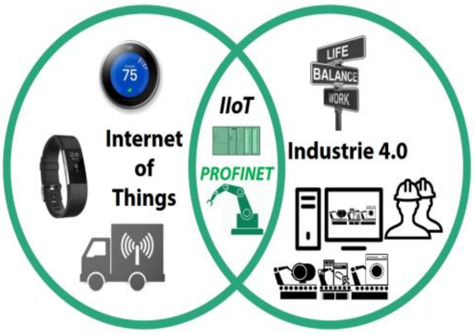
> *Many security problems associated with IIoT system, such as exposed ports, inadequate authentication practices, and obsolete applications, contribute to the emergence of risks.*

Risks to IIoT Systems: Many security problems associated with IIoT system, such as exposed ports, inadequate authentication practices, and obsolete applications, contribute to the emergence of risks. Insecure IIoT systems can lead to operational disruption and monetary loss. More connected environments indicate more security risks, such as:

- Software vulnerabilities that can be exploited to attack systems.
- Publicly searchable Internet-connected devices and systems.
- Malicious activities like hacking, targeted attacks, and data breaches.
- System manipulation that can cause operational disruption (e.g., product recalls) or sabotage processes (e.g., production line stoppage).
- System malfunction that can result in damage of devices and physical facilities or injury to operators or people nearby.

- OT systems held for extortion, as compromised through the IT environment.

Recommendation for Securing IIoT Systems: For IIoT systems, security by design and embedded security approach is more effective. A centralized Security Operation Centre (SOC) allows industries and enterprises to oversee the significant number of alerts which they may encounter and to enable quick response. Adopters of the IIoT could put emphasis on having a dedicated team for tackling security in an OT environment, given that it's a specialized area. Also having a full stack of protection purposely built into the different layers (the device, the network and the cloud) of IIoT implementations would enable industries and enterprises to securely conduct their operations. The device layer usually comprises the IIoT devices and applications that are brought in from different manufacturers and service providers. IIoT adopters should be able to know how their manufacturers and service providers transmit and store data. On the network area, there is the gateway, which gathers data from devices. This is the part where organizations should have next-generation Intrusion Prevention Systems (IPS) in order for them to monitor and detect potential attacks. Finally, the cloud is where providers should have security implementations that run server-based protection to mitigate the risk of hackers taking advantage of servers and stored data. Securing IIoT systems therefore requires connected threat defence, end to end protection from the gateway to the end point, which are able to provide:



Adopters of the IIoT could put emphasis on having a dedicated team for tackling security in an OT environment, given that it's a specialized area.

- Regular monitoring and detection in case of malware infection.
- Better threat visibility and early detection of anomalies.
- Proactive prevention of threats and attacks between IT and OT.
- Secure data transfer.
- A next-generation IPS to prevent attacks from exploiting vulnerabilities.
- Server and application protection across the data centre and the cloud.

References

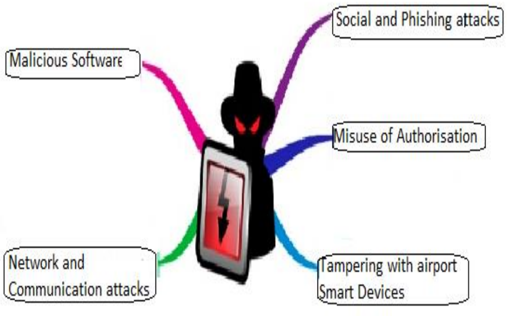
[1] https://en.wikipedia.org/wiki/Industrial_Internet_of_Things

[2] https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot

Cyber Threats in Aviation Industry

Sh. Abhijeet Raj Shrivastava and Sh. Jyoti Prakash, NCIIPC

India's National Air Space traffic is growing fast with schemes like Ude Desh Ka Aam Naagrik (UDAN), a Regional Connectivity Scheme of Government of India. This will continue to be a potential target for cyber-attacks. This may occur across the wide range of ICT systems, platforms and technologies that facilitate safe, resilient and efficient travel. There is a higher and ongoing risk of cyber-attacks or compromises that could cause disruption to aviation services in economic terms, commercial, operational and reputational also. Further, the risk of data theft and espionage may also be the reasons for such attacks. Cybersecurity is becoming a key enabler for safety, which is paramount in the aviation context. Major Cybersecurity threats against IoT applications in Aviation are as follows:


Malicious Software
Social and Phishing attacks
Misuse of Authorisation
Network and Communication attacks
Tampering with airport Smart Devices

Network and Communication Attacks: Smart Airports remain an attractive target of network attacks and various kinds of wireless communications, Air Traffic Management (ATM) and radio signals may be affected or jammed. Distributed Denial of Service attacks also enable attackers to disrupt information systems and networks, being able to impact on airport's system availability. As a result, there may be a serious impact on national economy and public safety.

There is a higher and ongoing risk of cyber-attacks or compromises that could cause disruption to aviation services in economic terms, commercial, operational and reputational also.

Faulty Business Continuity Planning and Disaster Recovery Implementation: A faulty BCP/DR implementation of Data Centres critical IT Business Process like software updates/ patches of core network elements may impact the overall functioning of the Airport Management Systems and can create chaos at major Airports.

Malicious Software: Malware, which is able to infect common information systems, airport's supervisory control and data acquisition systems. Systems not running the latest security patches are likely targets of malicious software attack.

Tampering with Airport Smart Devices: Airport devices can be tampered include manipulation of data at Central Reservation Systems, administration IT systems, Airport's stored sensor data. The threat of tampering also includes physical safety breaches and serious impact on Airport's security.

Airport employees, who lack security awareness and may not follow procedures, can pose a significant risk to airport cyber security.

Misuse of Authorization: Attackers may be able to obtain credentials and escalate authorization rights. Attackers can gain access, holding legitimate user's credentials; they can also escalate their privileges, and damage smart airport assets, depending on the level of privilege obtained.

Social and Phishing attacks: Airport employees, who lack security awareness and may not follow procedures, can pose a significant risk to airport cyber security. Phishing emails still may get through and trick the victim to perform a malicious action without knowing.

With continuous Vulnerability/Threat/Risk analysis (VTR) of the critical systems, attacks on these systems may be averted.

References

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/726561/aviation-cyber-security-strategy.pdf

[2] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6339064/

Guest Article

Quantum Safe Cryptography: Implications for Protection of NCII

Sh. Ramesh Singh, DDG (Retired) NIC

Sh. Ramesh Singh is IIT alumni and served the nation as Scientist in National Informatics Centre and Defence Research & Development Organisation. He is visiting faculty at IIT Delhi and Delhi Technical University. He has number of publications in national and international journals and conferences.

Abstract

Information is physical. The quantum paradigm provides intriguing basis for achieving computational power for certain class of mathematical problems that are completely intractable with the classical machine computations, as it stands today. One such computationally hard problem is public-key cryptography. Large scale Quantum Computing offers extraordinary opportunities and associated with it is a significant threat to the pervasive critical information infrastructure. The Quantum computers can crack even the most elaborate forms of encryption, including RSA and Elliptic Curve Cryptography in use today. The National Critical Information Infrastructure (NCII) will be at a higher risk of compromise once large-scale quantum computer has been built. Quantum Safe Cryptography is a set of new algorithms and techniques to help prevent Quantum attacks and safeguard NCII. It is therefore important to know the enablers of quantum safe cryptographic techniques along with the technical challenges to its deployment in existing systems and the impact of global standards.

Overview

The Rationale behind Quantum Safe Cryptography: The PKI algorithms RSA and ECC are synonymous with network security products and protocols, applications and services like Secure Software Distribution, Federated Authorization, Key Exchange over a Public Channel, Secure Email, VPN, SSL/TLS respectively, in an ubiquitous manner. PKI algorithms RSA, ECC, Diffie-Hellman and DSA are vulnerable to Quantum attacks and Shor's algorithms [1], can easily decipher the keys.

Quantum Safe Cryptographic Frameworks: The development of lattice theory, coding theory and the multivariate quadratic polynomials offer Quantum Resilient basis for the design of new PKI infrastructure and Quantum safe Ciphers with some trade-offs of lager Key Sizes and Signatures.

However these Quantum safe algorithms are performance wise competitive in nature. Wegman-Carter Authentication, Vernam's One Time Pad and specific variants of symmetric-key cryptography are information-theoretically secure and are resilient to Quantum attacks. Symmetric cipher defends itself against quantum adversary by simply doubling the key length. AES is believed to be quantum-safe. Similarly, well defined hash functions are resistant to quantum adversaries. The quantum-safe key establishment uses Quantum Key Distribution (QKD) based on Physics and Computational methods.

Symmetric cipher defends itself against quantum adversary by simply doubling the key length. AES is believed to be quantum-safe. Similarly, well defined hash functions are resistant to quantum adversaries. The quantum-safe key establishment uses Quantum Key Distribution (QKD) based on Physics and Computational methods.

Application Domains and Use Cases:

Following are the enumerated candidate use cases employing the technological infrastructures vulnerable to an adversary with a quantum computer:

- Encryption and authentication of endpoint devices
- Network infrastructure encryption
- Cloud Storage and computing
- SCADA systems

Application Domains:

- Protecting NCII
- BFSI Transactions Security
- Security of medical data and healthcare records
- Restricting access to confidential corporate networks
- Mobile Applications and Networks

Key Quantum Technologies

Quantum Algorithms: Quantum Algorithm employs intrinsic properties of quantum computation such as Quantum Superposition or Quantum Entanglement. The Shor's and Grover's algorithm are the two such developments. Shor's algorithm solves the discrete logarithm problem and the integer factorization problem in polynomial time [1]. Quantum Algorithms certainly threaten the widely deployed Cryptosystems. These algorithms employ Quantum Circuit model of computation which operates on Qubits as input and terminates with a measurement. There are other models like Hamiltonian Oracle Model where in Quantum Algorithms can be implemented.

Quantum Key Distribution (QKD): QKD deploys authenticated communication channel in tandem with a quantum communication channel in order to establish a secret key. Protocols for implementing quantum key distribution require both a quantum channel and free space to send quantum states of light, and an authenticated classical channel for the sender [2].

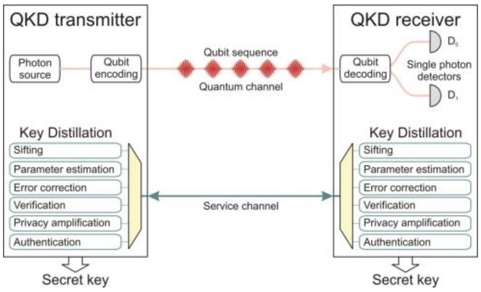


Illustration of a typical prepare-and-measurement QKD setup [2]

QKD is definitely a secure key distribution mechanism for quantum safe symmetric key algorithms like Advanced Encryption Standard (AES), or one-time pad encryption to be hacker proof.

First Large Scale Deployment of QSC based QKD to Critical Energy Information Infrastructure

QKD systems produce perfect random keys nearly impossible to be deciphered by modern day computers. QKD helps detection of eavesdropping. QKD is a Quantum Technology and an enabler for a "Scalable Quantum Cryptography Network for Protected Automation Communications" [3], a flagship research and development initiative of US Department of Energy, providing QKD to critical energy infrastructure, where in QKD components have been designed, the prototypes fabricated and the technology deployed and due for demonstration during the year 2019 [3]. QKD network provides security by using entangled photon. Open-Source Protocol SSP-21 provide methods for receiving and using the keys designed for utility ICS networks, compatible with QKD keys. The GRID Cyber Security improves due to provisioning of uncrackable, self-managing cryptographic keys with channel temper detection [3].

QUANTUM SAFE
NO CERTIFICATE AUTHORITY
LONG-TERM SOLUTION
SECURE
TAMPER DETECTING
NO PKI
NO I.T. OVERSIGHT
SIMPLE
LOW LATENCY
NO KEY STORAGE
PROTOCOL COMPATIBLE

QKD benefits to utility networks

Technical Challenges

Requirement of compact and stable entangled photon sources, third-party Integration and Fibre Loss Management are the key challenges to be confronted [3].

References

[1] Shor, P. W. (1997). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". SIAM Journal on Scientific and Statistical Computing. 26 (5): 1484–1509. arXiv: quant-ph/9508027. Bibcode:1995quant.ph..8027S. doi:10.1137/s0097539795293172

[2] https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

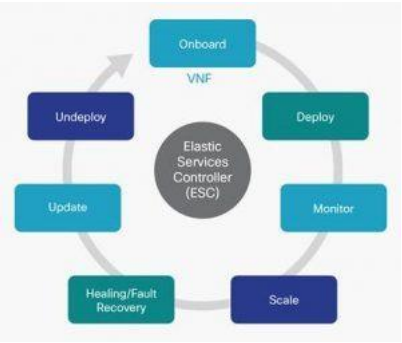
[3] https://www.energy.gov/sites/prod/files/2018/12/f58/Qubitekk%20-%20Scalable%20Quantum%20Cryptography%20Network.pdf

Vulnerability Watch

Critical Flaw in Cisco Elastic Services Controller

Source: https://tools.cisco.com/

A vulnerability ranked "critical" was found in the REST API of Cisco Elastic Services Controller (ESC). Cisco Elastic Services Controller is a virtual network functions manager, which enables businesses to automate the deployment and monitoring of functions running on their virtual machines. The authentication bypass vulnerability, CVE-2019-1867, has a CVSS score of 10 out of 10, making it a critical flaw. This issue could allow an unauthenticated, remote attacker to bypass authentication on the REST API, potentially enabling an attacker to execute arbitrary actions through the REST API with administrative privileges on an affected system. The vulnerability is due to improper validation of API requests. An attacker could exploit this vulnerability by sending a crafted request to the REST API. This vulnerability affects Cisco Elastic Services Controller running Software Release 4.1-4.4 when the REST API is enabled. The REST API is not enabled by default. Cisco has released software updates that address this vulnerability.



The authentication bypass vulnerability, CVE-2019-1867, has a CVSS score of 10 out of 10, making it a critical flaw.

Access Control Bypass Vulnerability in Envoy Proxy

Source: https://nvd.nist.gov/

Access Control Bypass Vulnerability (CVE-2019-9901) in Envoy could allow an unauthenticated, remote malicious user to bypass security restrictions and conduct directory traversal attacks. The vulnerability exists because the affected software fails to normalize HTTP URL paths. An attacker could exploit this vulnerability by submitting a crafted URL to the targeted system. It has a CVSS 3.0 Base Score of 10.0. Envoy Proxy has released software updates.

envoy
ENVOY IS AN OPEN SOURCE EDGE AND SERVICE PROXY, DESIGNED FOR CLOUD-NATIVE APPLICATIONS

Command Injection Vulnerability in IBM API Connect

Source: https://nvd.nist.gov/

A critical vulnerability (CVE-2019-4202) has been found in IBM API Connect 5.0.0.0/5.0.8.6. Affected is an unknown function of the component Developer Portal. An attacker with a specially crafted request can run arbitrary code on the server and gain complete access to the system. The manipulation with an unknown input leads to a privilege escalation vulnerability (Command Injection). It has a CVSS 3.0 Base Score of 10.0. IBM has released software updates that address this vulnerability. IBM Security Bulletin 880109 refers to patch, upgrade or suggested workaround information of this vulnerability.

Critical Vulnerability found in Ctrip Apollo

Source: https://cve.mitre.org/

SSRF vulnerability has been found in Ctrip Apollo (CVE-2019-10686). This vulnerability was found in an API from Ctrip Apollo through 1.4.0-SNAPSHOT. An attacker may use it to do an intranet port scan or raise a GET request via /system-info/health because the %23 substring is mishandled. As an impact it is known to affect confidentiality, integrity, and availability. It has a CVSS 3.0 Base Score of 10.0.

Critical Vulnerability in Red Hat Ansible Fetch Module

Source: https://www.securityfocus.com/bid/107650

A path-traversal vulnerability (CVE-2019-3828) has been found in Ansible fetch Module before versions 2.5.15, 2.6.14 and 2.7.8. This vulnerability allows a local attacker to conduct a path traversal attack on a targeted system, which can be used to access or modify sensitive information. The vulnerability exists in the lib/ansible/action/__init__.py source code file of the affected software, and is due to improper restriction of an absolute path, which could cause the fetch module to copy and overwrite files outside of the specified directory destination on an affected system. An attacker could exploit this vulnerability by persuading a user to access a link that submits malicious input to the targeted system. To exploit this vulnerability, the attacker must have user-level access to the targeted system. This access requirement could reduce the likelihood of a successful exploit. Red Hat confirmed the vulnerability and released software updates.

This vulnerability allows a local attacker to conduct a path traversal attack on a targeted system, which can be used to access or modify sensitive information.

Vulnerability in Timelion Visualizer Component of Elastic Kibana

Source: https://nvd.nist.gov/

Kibana is an open source data visualization plugin for Elasticsearch. It provides visualization capabilities on top of the content indexed on an Elasticsearch cluster. A critical vulnerability (CVE-2019-7609) in the Timelion visualizer component of Elastic Kibana has been found. The vulnerability exists because the affected software mishandles user-supplied input. An attacker could exploit this vulnerability by sending requests that submit malicious input to the affected software. A successful exploit could allow the attacker to execute arbitrary JavaScript code on the system. Elastic confirmed the vulnerability and released software updates.

The vulnerability exists because the affected software mishandles user-supplied input.

Server Side Request Forgery Flaw in Moodle

Source: https://security-tracker.debian.org/tracker/CVE-2019-3809

Moodle is a free and open-source learning management system written in PHP. A critical vulnerability (CVE-2019-3809) has been found in the mybackpack functionality of Moodle that could allow an unauthenticated, remote attacker to conduct a Server Side Request Forgery (SSRF) attack on a targeted system. This vulnerability exists because Moodle incorrectly allows the setting of badge URLs. An attacker could exploit this vulnerability by submitting requests to the affected software. Administrators are advised to allow only trusted users to have network access.

GitLab Community allows SSRF

Source: https://cve.mitre.org

GitLab offers powerful integration with Prometheus for monitoring key metrics of apps, directly within GitLab. Metrics for each environment are retrieved from Prometheus, and then displayed within the GitLab interface. The Prometheus integration feature of GitLab was vulnerable to SSRF which could result access to internal services. The issue is mitigated in the latest release and is assigned CVE-2019-9174. It has a CVSS 3.0 Base Score of 10.0.

Access Issue with Additional Sandbox Restriction

Source: https://www.tenable.com/cve/CVE-2018-4310

Sandboxing is a great way to protect systems and users by limiting the privileges of an app to its intended functionality, increasing the difficulty for malicious software to compromise user systems. An access issue was addressed with additional sandbox restrictions. This issue affected versions prior to iOS 12 and macOS Mojave 10.14. Impact of this vulnerability is that a sandboxed process may be able to circumvent sandbox restrictions. This issue was assigned CVE-2018-4310 with CVSS 3.0 Base score of 10.0.

Install macOS Mojave

macOS Mojave

To set up the installation of macOS Mojave, click Continue.

Memory Corruption Vulnerability in Multiple Apple Products

Source: https://www.securityfocus.com/bid/106724/solution

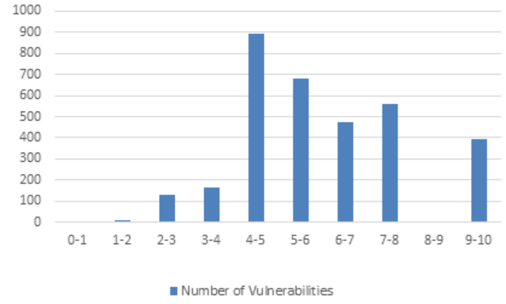
Apple iTunes/macOS/tvOS/watchOS/iOS are prone to memory-corruption vulnerability (CVE-2019-6235). The issue was addressed with improved validation. It has a CVSS 3.0 Base Score of 10.0. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3, and iTunes 12.9.3 for Windows. An attacker can leverage this issue to execute arbitrary code with system privileges. Failed exploit attempts will likely result in denial-of-service conditions.

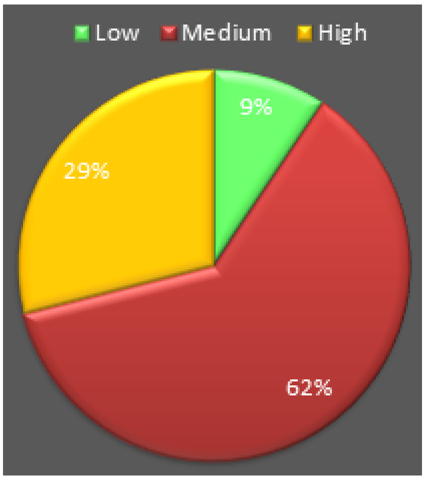
An attacker can leverage this issue to execute arbitrary code with system privileges.

Quarterly Vulnerability Analysis Report

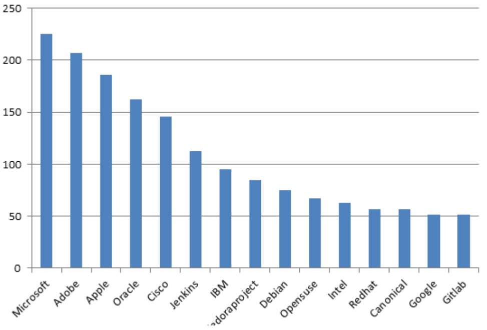
Sh. Sandeep Kumar and Ms. Rup Shikha, NCIIPC

A total of 3314 vulnerabilities were observed from the month of March-May 2019. Most of the vulnerabilities had a score ranging from 4-6. 62 percent of total vulnerabilities reported were of medium severity. Microsoft, Adobe, Apple, Oracle and Cisco were the top five vendors sharing around 28 percent of total reported vulnerabilities. [1]





Severity	Score	Number of Vulnerabilities			Total	
		March	April	May		
Low	0-1	-	1	2	3	310
	1-2	3	8	2	13	
	2-3	30	60	41	131	
	3-4	32	69	62	163	
Medium	4-5	95	474	323	892	2045
	5-6	94	314	273	681	
	6-7	75	245	152	472	
High	7-8	96	228	235	559	959
	8-9	1	1	2	4	
	9-10	32	137	227	396	
Total		458	1537	1319		3314



S. No.	Vendor	March	April	May	Total
1.	Microsoft	8	137	80	225
2.	Adobe	0	0	207	207
3.	Apple	0	186	0	186
4.	Oracle	2	159	1	162
5.	Cisco	25	30	91	146
6.	Jenkins	14	93	6	113
7.	IBM	13	55	27	95
8.	Fedoraproject	38	39	8	85
9.	Debian	41	27	7	75
10.	Opensuse	45	19	3	67
11.	Intel	32	3	28	63
12.	Redhat	27	26	4	57
13.	Canonical	21	36	0	57
14.	Google	0	22	29	51
15.	Gitlab	2	22	27	51

References

[1] https://www.cvedetails.com

Security App

Google Open Sources its Sandboxed API

Source: https://www.securityweek.com

It's not uncommon for applications to be affected by memory corruption or other types of vulnerabilities that can be exploited for remote code execution and other purposes. Using a sandbox ensures that the code responsible for processing user input can only access the resources it needs to, which mitigates the impact of a flaw by containing the exploit to a restricted environment and preventing it from interacting with other software components. While sandboxing can be highly useful, Google says it's often not easy to implement. That is why the internet giant has decided to open source its Sandboxed API, which should make it easier to sandbox C and C++ libraries. The company has also open sourced its core sandboxing project, Sandbox2, which can be used on its own to secure Linux processes. The Sandboxed API and Sandbox2 source code is available on GitHub, along with usage instructions.

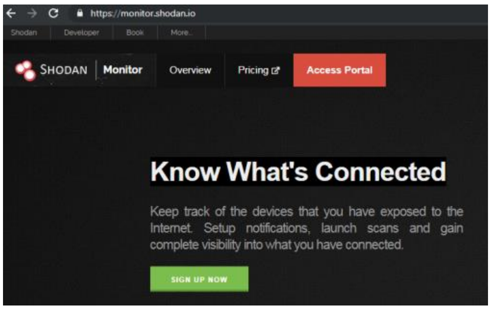
Image Source: https://www.questechie.com/

The Sandboxed API and Sandbox2 source code is available on GitHub, along with usage instructions.

Shodan Monitor helps Users to setup Network Alerts

Source: https://cyware.com/, https://hub.packtpub.com/

Shodan, the IoT search engine launched a new service called Shodan Monitor that helps users to setup network alerts and keeps a track of what's connected to the Internet. It helps in detecting leaks to the cloud, identifying phishing websites and compromised databases. Users will be able to explore what they have connected to the Internet within their network range. The users can also set up real-time notifications in case something unexpected shows up. Shodan Monitor is free for existing customers; the service is also reachable via the Shodan API and the command-line interface.



Know What's Connected

Keep track of the devices that you have exposed to the Internet. Setup notifications, launch scans and gain complete visibility into what you have connected.

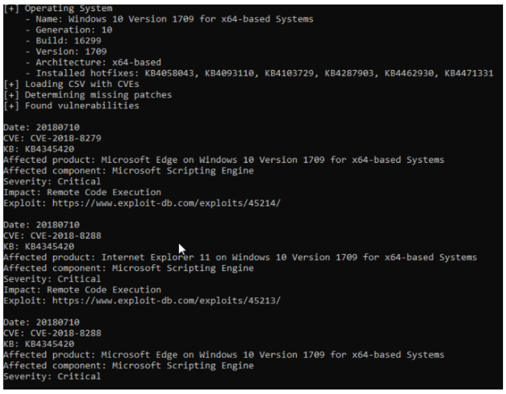
Ghidra - A Reverse Engineering Framework developed by NSA

Source: https://www.nsa.gov/resources/everyone/ghidra/

Ghidra is a reverse engineering framework developed by the United States National Security Agency (NSA) Research Directorate for its cybersecurity mission. It helps in analysing malicious code and can help in better understanding of potential vulnerabilities in the networks and systems. NSA released a free, public version of Ghidra along with its source code. This source code repository includes instructions to build on all supported platforms (macOS, Linux, and Windows). With this release, developers will be able to collaborate by creating patches, and extending the tool to fit their cybersecurity needs.

WES lists all unpatched vulnerabilities on Computer

Source: https://github.com/bitsadmin/wesng



```
[+] Operating System
    - Name: Windows 10 Version 1709 for x64-based Systems
    - Generation: 10
    - Build: 16299
    - Version: 1709
    - Architecture: x64-based
    - Installed hotfixes: KB4058043, KB4093110, KB4103729, KB4287903, KB4462930, KB4471331
[+] Loading CSV with CVEs
[+] Determining missing patches
[+] Found vulnerabilities

Date: 20180710
CVE: CVE-2018-8279
KB: KB4345420
Affected product: Microsoft Edge on Windows 10 Version 1709 for x64-based Systems
Affected component: Microsoft Scripting Engine
Severity: Critical
Impact: Remote Code Execution
Exploit: https://www.exploit-db.com/exploits/45214/

Date: 20180710
CVE: CVE-2018-8288
KB: KB4345420
Affected product: Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Affected component: Microsoft Scripting Engine
Severity: Critical
Impact: Remote Code Execution
Exploit: https://www.exploit-db.com/exploits/45213/

Date: 20180710
CVE: CVE-2018-8288
KB: KB4345420
Affected product: Microsoft Edge on Windows 10 Version 1709 for x64-based Systems
Affected component: Microsoft Scripting Engine
Severity: Critical
```

Windows Exploit Suggester - Next Generation (WES-NG) is a tool based on the output of Windows' systeminfo utility and provides with the list of vulnerabilities the Windows Operating System (OS) is vulnerable to, including any exploits for these vulnerabilities. It works by comparing Windows SystemInfo report with a downloaded CSV file of known vulnerabilities and their associated security updates. Using this data, Windows Exploit Suggester displays a report showing all the unpatched vulnerabilities found on the computer and their respective CVE IDs, Microsoft knowledge base article numbers, and a link to any known exploits for that vulnerability. It supports every Windows OS between Windows XP and Windows 10, including their Windows Server counterparts.

NCIIPC Initiatives

NCIIPC at Cyber Security Conference for Hydro Sector

Sh. Balraj Joshi, CMD, NHPC addressing participants of conference

Sh. Sanjeev Chawla, DDG NCIIPC and Sh. R.K. Singh, Director NCIIPC delivered talk on "Critical Information Infrastructure Identification and Cyber Security in Power Sector".

NHPC Limited has been nominated by Ministry of Power to establish CERT-Hydro and given the responsibility of providing guidance and support to hydro-sector CPSUs, State and Private Utilities for establishing their Cyber Security Framework. A one-day Cyber Security Awareness Conference was organized by NHPC on 24 Jun 2019 at Taj Vivanta, Faridabad Haryana. The conference was attended by CISOs of Hydro constituent organizations. There were guest speakers from NCIIPC, Ministry of Power, CERT-in and Industrial Cyber Security experts from DSCI, Ernst & Young etc. Critical Information Infrastructure Identification, Cyber Security in Power Sector, Cyber Security for ICS/SCADA Systems, ISMS 27001: 2013 and IIoT Security were the major topics for discussion. Sh. Sanjeev Chawla, DDG NCIIPC and Sh. R.K. Singh, Director NCIIPC delivered talk on "Critical Information Infrastructure Identification and Cyber Security in Power Sector". The conference was attended by the representatives of 25 Hydro sector utilities across India.

One Day Workshop by NCIIPC for Ministry of Civil Aviation

A One-day workshop was organised by NCIIPC in association with Airport Authority of India (AAI) for all attached offices of Ministry of Civil Aviation on 22nd May 2019 at Indian Aviation Academy, New Delhi.

Sh. Sanjeev Chawla, DDG and NCIIPC team imparted training on formulation of Information Security Policy, Identification of Critical Information Infrastructure, various SOPs of NCIIPC and Cyber security awareness. The officials from Ministry of Civil Aviation, AAI, Air India, Pawanhans, DGCA, AAIB and IT experts from different airports attended the workshop. Following were the major topics covered during the workshop:

- Roles and responsibilities of NCIIPC
- Cyber Security Hygiene and Best Practices
- Cyber Security Evaluation for CII and Information Security Formulation

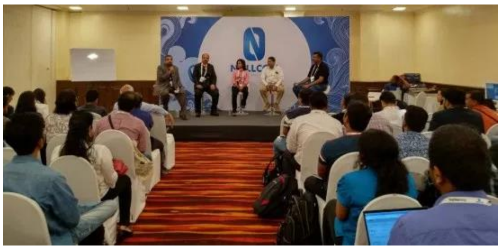
भारतीय विमानन अकादमी
Indian Aviation Academy
One day information security workshop
On 22nd May 2019 at IAA, New Delhi.

Participants of one-day workshop organised by NCIIPC for Ministry of Civil Aviation

NCIIPC at Nullcon Goa 2019

Source: https://www.youtube.com/, https://www.medianama.com/

NCIIPC participated in Nullcon Goa 2019 organised during 26 Feb - 2 Mar 2019. Nullcon is Asia's Premier Information Security Conference & Training platform for security & privacy practitioners, executives, academia & enthusiasts. NCIIPC participated in boardroom discussion on "How to respond to Breaches". Sh. Sachin Burman, DDG NCIIPC highlighted the importance of having processes in place for detection, containment and mitigation of the attacks. He discussed about the NCIIPC initiatives of Responsible Vulnerability Disclosure Program and Incident Response mechanism. He also created awareness about the new emerging trends of attacks on Industrial Control Systems.



CXO Panel: Breached? – Here Is How I Responded! | nullcon Goa 2019

A Two Day DTF Event for BFSI Sector at Mumbai

NCIIPC along with Information Sharing and Analysis Centre (ISAC) organised a two day DTF event for BFSI Sector at Mumbai on 27-28 June 2019. The event was attended by top decision makers from BFSI sector to discuss cybersecurity challenges and best practices to enhance cyber resilience across India.

Sh Lokesh Garg, Director NCIIPC addressing the participants at two day DTF event for BFSI sector at Mumbai

NCIIPC Responsible Vulnerability Disclosure Program

http://nciipc.gov.in/RVDP.html

The NCIIPC Responsible Vulnerability Disclosure Program provides opportunity for researchers to disclose vulnerability observed in Nation's Critical Information Infrastructure. NCIIPC acknowledges the following researchers for their contributions towards disclosure of vulnerabilities for protection of National Critical Information Infrastructure:

- Ashutosh Barot
- Shaikh Arshe Azam
- Acelakshit Verma

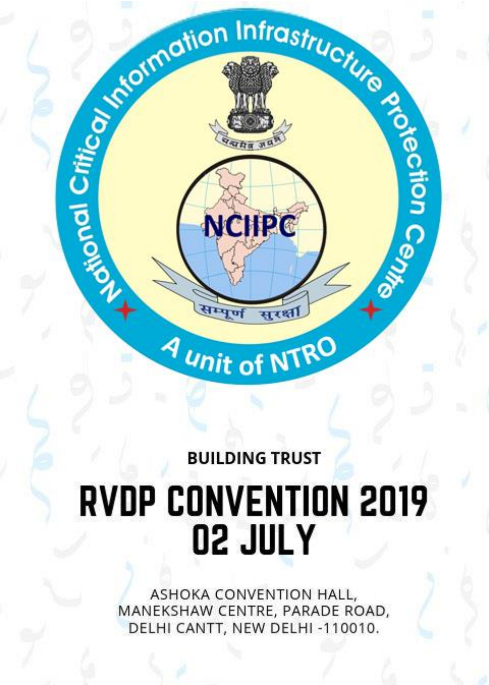
NCIIPC acknowledges the researchers for their contributions towards protection of National Critical Information Infrastructure.

- Adesh Kolte
- Aditya Shende
- Ajay Shrimali
- Akash Labade
- Akshaey Bhosale
- Amiya Behera
- Anantha Krishnan.E.R
- Arpit Borawake
- Aseem Jakhar
- Bagus Wiratma Adi
- Bathini Vijaysimha Reddy
- Bhavesh Thakur
- Chetan Tiwari
- Damini Soni
- Dhruv Mankad
- ErodeDCCB Erode
- Geethu Sivakumar
- Gregorius Aprisunnea
- Harsh Joshi
- Jayati soni
- Jayesh Baviskar
- Joby Daniel
- Junaid farhan
- kolta88@gmail.com
- Lalit Choudhary
- mru bugbounty
- Mukesh Kumar Rao
- Naiju Nandan
- Navoneel Jana
- Nilesh Dalavi
- Nishant Pawar
- Parag Gupta
- Pranay Bafna
- Pranshu Tiwari
- Pritam Das
- Prosirius Technologies
- Raju Kumar
- Raghav Sharma
- Rahul Batra
- Rakshith (@vrisha_karna)
- Ram Prasad. Uppada
- ran hackers
- research@talosinfinite.com
- Sachin Gupta
- Sameera Fatima
- Sangramsinh Pawar
- Sarthak Goyal
- Saurabh Kumar Pandey

- Savan
- sf8882020@gmail.com
- shankar acharya
- Shantanu Kulkarni
- Shashank Chaurasia
- Shiv Charan Kataria
- Shreekanth Pillai
- Shubham Nagar
- Shushma Ahuja
- Sourajeet Majumder
- Sreedeep.Ck Alavil
- Subhamoy Guha
- Suresh Prasanna
- Sushmitha Katikitala
- tab nexa
- Tijo Davis
- Tolesh Kumar Jangid
- Tufail Ahmad
- Tushar Shinde
- Udit Bhadauria
- Umesh Jore
- Urvesh Thakkar
- Varsha Choudhary
- Varun Thorat
- Vishal Bharad
- Vishnu Prasad P G
- Yash Mehta

NCIIPC RVDP Convention

NCIIPC is grateful to the Responsible Vulnerability Disclosure Programme contributors of NCIIPC, the proactive nature of which has actively prevented various potential cyber-attacks. NCIIPC organised a one day RVDP Convention (by invitation only) on 2nd July 2019 at Manekshaw Centre, New Delhi to acknowledge the contributions of the researchers.

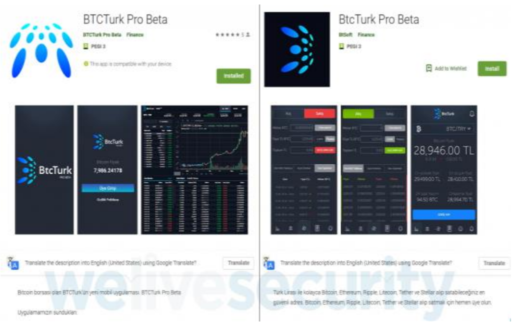

National Critical Information Infrastructure Protection Centre
सत्यमेव जयते
NCIIPC
सम्पूर्ण सुरक्षा
A unit of NTRO

BUILDING TRUST

RVDP CONVENTION 2019
02 JULY

ASHOKA CONVENTION HALL,
MANEKSHAW CENTRE, PARADE ROAD,
DELHI CANTT, NEW DELHI -110010.

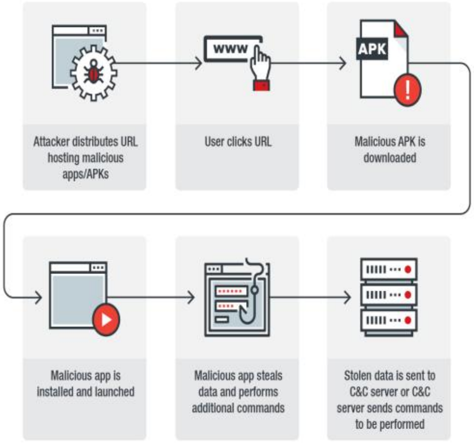
Mobile Security



Malicious Android apps targeting BtcTurk Exchange

Source: https://www.welivesecurity.com

A series of malicious apps has recently been uploaded in Google Play store, capable of accessing one-time-passwords (OTPs) in SMS 2FA messages without using SMS permission. These apps tried to impersonate the official app of BtcTurk which is a Turkish crypto-currency exchange. The first of the apps was uploaded under the name 'BTCTurk Pro Beta' by the developer named 'BTCTurk Pro Beta' followed by the app 'BtcTuck Pro Beta' by 'BtSoft'. Even after removal of these two apps from Google Play store as reported by ESET, a third app with the same name as 'BTCTURK PRO' was uploaded. After installation, the app asks for 'Notification access' permission and when the user grants it, the app displays a fake login page of BtcTurk which requests the user to provide his/ her credentials. After submission of credentials, a fake error message is displayed and, in the background, the credentials along with the OTP caught from notifications appearing on the compromised device's display, is sent to the hacker.


Attacker distributes URL hosting malicious apps/APKs
WWW
User clicks URL
APK
Malicious APK is downloaded
Malicious app is installed and launched
Malicious app steals data and performs additional commands
Stolen data is sent to C&C server or C&C server sends commands to be performed

Bouncing Golf targeting Middle Eastern Countries

Source: https://blog.trendmicro.com

According to Trend Micro, a cyber-espionage campaign named 'Bouncing Golf' is targeting Middle Eastern countries. It is detected as AndroidOS_GolfSpy.HRX which has a vast range of cyber-espionage capabilities. As far as 660 android devices are infected by this and information stolen are mostly of military related. The malware is capable of stealing device accounts, current running processes, call logs, clipboard contents, device location, files from SD card etc. The app is also found to be connected to a remote server for performing command-based attacks on its victims.

2019
RAM Master - Memory Optimizer
Pic Tools Group (Photo Editor& Photo Grid&Collage)
Tools
404,594
PEGI 3
Contains Ads
Add to Wishlist
Install
PHONE BOOSTER
maximize your phone speed
CPU COOLER
freeze overheating apps
BATTERY SAVE
stop battery draining process
JUNK C
remove

PreAMo targeting Advertisement agencies

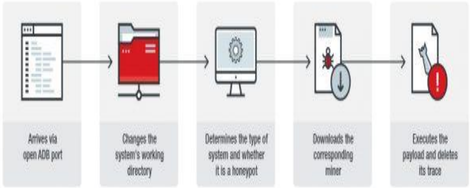
Source: www.buzzfeednews.com, research.checkpoint.com

Buzzfeed News has recently discovered a large number of popular android apps developed by a Chinese developer named 'DO Global' is behind a large-scale advertisement fraud operation. Six of their popular apps with over 90 million downloads have been found fraudulently clicking on ads to generate revenue. The malware 'PreAMo' found here has been imitating users to click on banners received from three ad agencies namely Presage, Admob and Mopub. The malware is found to be communicating with a C&C server (res.mnexuscdn.com).

Malware leveraging on ADB and spreading via SSH

Source: https://blog.trendmicro.com

Trend Micro has recently discovered a crypto-currency mining botnet malware which arrives at an ADB running device via an IP address: 45.67.14.179 and then executes a script to download its payload. By executing the payload, the attacker gets infected system's information and points to the address http://198.98.51.104 containing three miners where one of the miners is used in order to execute further command to compromise the host. It can also then spread from the infected host to others using the previous SSH connections of the host.


Arrives via open ADB port
Changes the system's working directory
Determines the type of system and whether it is a honeypot
Downloads the corresponding miner
Executes the payload and deletes its trace

Improved Security features in Android Q

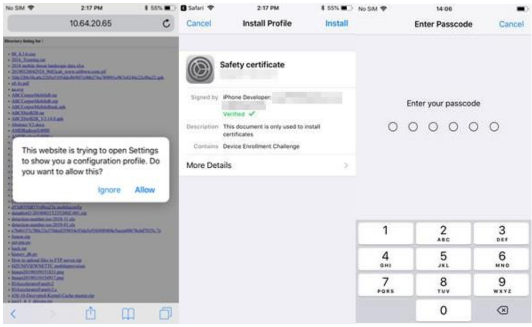
Source: https://android-developers.googleblog.com

Three important security measures coming with Android Q have been mentioned in Google I/O 2019. The first one is Adiantum which is a storage encryption mechanism requiring no cryptographic acceleration hardware and also, TLS 1.3 support is enabled by default in Android Q. The second one is platform hardening which includes sandbox for software codecs, Shadow Call Stack, protecting Address Space Layout Randomization (ASLR) against leaks using eXecute-Only Memory (XOM), Scudo hardened allocator etc. The third one is the updating of underlying framework for BiometricPrompt API introduced in Android Pie, with robust support for face and fingerprint which includes additional use-cases of both implicit and explicit authentications. Google is also looking to add Electronic ID support for mobile apps via which one can use his/ her device as an ID, for example Driver's license.

New variant of XLoader emerges

Source: https://blog.trendmicro.com

A new variant of XLoader has been spotted by Trend Micro which poses as a security app in Android Devices and uses a malicious iOS profile to infect iPhone and iPad devices. It has been termed as XLoader version 6.0 or AndroidOS_XLoader.HRXD. Here the attackers have used several fake websites and lured users into downloading fake APKs from these websites. There has also been report of smishing. In case of Apple devices, the users are lured to install a malicious iOS configuration profile. The profile then is used to lure the victim to an Apple phishing site and gather UDID, IMEI, ICCID, MEID, version number, product number of his/ her device. It has also been assumed to have a connection to another android malware named 'FakeSpy' which targeted Japanese and Korean-speaking users.



This website is trying to open Settings to show you a configuration profile. Do you want to allow this?

Ignore Allow

Safety certificate

Signed by: iPhone Developer:

Verified ✓

Description: This document is only used to install certificates

Contains: Device Enrollment Challenge

More Details

Enter your passcode

○ ○ ○ ○ ○ ○

Upcoming Events - Global

July 2019

Cyber-Physical System Security Workshop, Auckland	8 Jul
5th VDI Conference – Cyber Security for Vehicles, Dusseldorf, Germany	9 Jul
FutureCon - Detroit, Michigan, United States	10 Jul
Minneapolis Cybersecurity Conference, Minneapolis, Minnesota, USA	11 Jul
Cyber Security Summit: DC Metro, McLean, Virginia	16 Jul
RSA Conference 2019 Asia Pacific & Japan, Singapore	16-18 Jul
Raleigh Cybersecurity Conference, Raleigh, USA	18 Jul

JULY 2019

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

August 2019

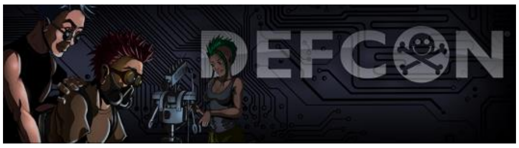
SecureCISO Dallas, Texas	1 Aug
Gartner Security & Risk Management Summit, Tokyo, Japan	5-7 Aug
Cyber Security in Government, Canberra, Australia	6 Aug
DEF CON 27, Las Vegas	8-11 Aug
PCI Security Standards 2019 Latin America Forum, São Paulo, Brazil	15 Aug
InfoSec Healthcare Connect 2019, Fort Lauderdale, Florida	19-21 Aug
SecureCISO Toronto, Ontario	22 Aug

AUGUST 2019

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

September 2019

Global CISO Executive Summit, Westlake Village, California	9-11 Sep
Global AppSec – DC, Washington	9-13 Sep
Oil & Gas Cybersecurity Summit & Training 2019, Houston, Texas	16-22 Sep
R3: Resilience, Response & Recovery Summit 2019, London	17 Sep
Industry 4.0 - Industrial Cyber Security and Industrial IoT, Chicago, Illinois, USA	23-24 Sep
Cyber Security for Critical Assets APAC, Singapore	25-26 Sep
Threat Hunting & Incident Response Summit & Training 2019, New Orleans, Louisiana	30 Sep-7 Oct



October 2019

• Cyber Security Summit New York 2019	3 Oct
• Pittsburgh CISO Executive Summit	9 Oct
• International Conference on System Safety and Cyber Security, London	21-22 Oct
• Industrial Control Systems Cyber Security Conference, Atlanta	21-24 Oct
• Transforming Controls Safety and Security – How Safe is your Asset?, United Kingdom	30 Oct

12
cocon
Hacking and Cyber Security Briefing
12th Edition
Sep 25-28, 2019 - Grand Hyatt, Kochi (Cochin) Kerala, India

Upcoming Events - India

• NCIIPC RVDP Convention 2019, New Delhi	2 Jul
• Annual IoT and AI Summit, Bengaluru	3 Jul
• INBA General Counsel Summit 2019, Mumbai	19 Jul
• Best Practices Meet 2019, Bengaluru	24-25 Jul
• Smart Tech BFSI Leaders' Meet, Bengaluru	7 Aug
• Gartner Security & Risk Management Summit 2019, Mumbai	26-27 Aug
• SANS Hyderabad 2019	26-31 Aug
• Cyber Security Conference, Hyderabad	4-5 Sep
• c0c0n 2019 Hacking and Cyber Security Briefing, Kochi	25-28 Sep
• Nullcon Security Training, Delhi	9-10 Oct
• BSides Delhi	11 Oct
• Cyber Security Summit 2019 – Bangalore	11 Oct
• HAKON – International Information Security Meet, Indore	13 Oct
• SANS Mumbai 2019	4-9 Nov

SEPTEMBER 2019

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

OCTOBER 2019

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

NCIIPC RVDP Convention 2019

02 July 2019

Ashoka Convention Hall
Manekshaw Centre, Parade Road
Delhi Cantt, New Delhi -110010

N
ULLCON SECURITY TRAINING: 9 - 10 OCTOBER 2019
VENUE: VIVANTA BY TAJ, DELHI

General Help		helpdesk1@nciipc.gov.in helpdesk2@nciipc.gov.in
Incident Reporting	:	ir@nciipc.gov.in
Vulnerability Disclosure	:	rvdp@nciipc.gov.in
Malware Upload	:	mal.repository@nciipc.gov.in
NCIIPC Newsletter	:	newsletter@nciipc.gov.in

Notes

National Critical Information Infrastructure Protection Centre

सत्यमेव जयते

NCIIPC

सम्पूर्ण सुरक्षा

A unit of NTRO

Feedback/Contribution

Suggestions, feedback and contributions are welcome at
newsletter@nciipc.gov.in

Copyright
NCIIPC, Government of India

Disclaimer
NCIIPC does not endorse any vendor, product or service. The content of the newsletter is for informational purpose only. Readers may validate the information on their own.