NEWSLETTER

April 2019

National Critical Information Infrastructure Protection Centre

A unit of National Technical Research Organisation

VOLUME 3 ISSUE 2

@NCIIPC

NCIIPC Newsletter

April 2019

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

The announcement of the forthcoming General Elections in India brings to fore the global concerns on security of the election infrastructure. There is no gainsaying that Social Media plays an important role in the campaigns. There is a looming threat of influencing the elections by the inimical countries. The incidents of hacking of emails of various parliamentary parties in various elections round the globe highlight the need to formulate a concrete strategy in this direction. The introduction of Global Electoral Exchange Program in US to promote international exchanges on best election practices and cultivate more secure democratic institutions around the world is a welcome step.

Past few months have seen increased incidents of Domain Name Server (DNS) hijacking. Attempted infections by malware designed to steal money via online access to bank accounts were logged on large number of computers. Trends also indicate that Ransomware is gradually declining and being replaced with Crypto-mining Malware having the potential to steal computer resources and discreetly mine for crypto-currency. The suspected involvement of some nation state actors cannot be ruled out.

Considering the threats, the United States Department of Homeland Security has issued an emergency directive. Russia is considering the options of cutting off from the Global Internet temporarily. It is the need of the hour to ensure order and take steps to maintain integrity, resilience and safety of the cyber world.

NCIIPC in making constant endeavour to sensitise the stakeholders of Critical Sectors by conducting awareness workshops, seminars and 'Defend the Flag' events across the country. NCIIPC also participated in and sponsored various national, International and academic events.

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

News Snippets - National

PM Emphasized on Capacity Building in Police on Cyber Security

Source: https://www.narendramodi.in

Prime Minister of India, Sh. Narendra Modi, addressed the Valedictory Ceremony at the Conference of Director Generals and Inspector Generals of Police at Kevadiya in Gujarat. He appreciated the officers for looking at all issues in the national perspective. The Prime Minister stressed on the importance of Inter-State coordination, in tackling crime. He called upon senior officers to work towards greater recognition of police personnel who work for the benefit of the people. Social media can be used effectively for this purpose. Prime Minister emphasized on the need for capacity building in police forces, on the subject of cyber security. He launched the portal of the Cyber Coordination Centre. This is envisaged as an umbrella platform that will help Law Enforcement Agencies coordinate their efforts to solve all cybercrimes and incidents.

Prime Minister emphasized on the need for capacity building in police forces, on the subject of cyber security.

Home Minister Inaugurated the National Cyber Forensic Lab

Source: https://coingeek.com

Union Home Minister, Sh. Rajnath Singh, inaugurated the newly-created National Cyber Forensic Lab (NCFL), which is tasked with investigating and resolving crypto-related crimes, as well as other types of cyber fraud. The NCFL is expected to have a division specifically dedicated to the fighting crypto crimes. In addition to the NCFL, Delhi will also have a new Cyber Protection Awareness and Detection Centre (CyPAD). New Delhi Police Commissioner Amulya Patnaik explains, "We are now equipped with technology to recover data from damaged hard disks, cryptocurrency analysis, malware forensic and data can be retrieved from 33,000 kinds of mobile models available in the market." Included under the umbrella of the NCFL are other units, such as a Memory Forensics Lab, an Image Enhancement Lab, a Network Forensics Lab, an Advanced Mobile Forensics Lab and a Damaged Hard Disk Cryptocurrency Forensics Lab.

"We are now equipped with technology to recover data from damaged hard disks, cryptocurrency analysis, malware forensic and data can be retrieved from 33,000 kinds of mobile models"

Cybersecurity Framework for Stock Brokers and Depository Participants

Source: https://www.moneycontrol.com/

Securities and Exchange Board of India (SEBI) put in place a cybersecurity framework for stock brokers and depository participants amid concerns over possible data breaches. With the new norms, to be effective from April 2019, stock brokers and depository participants would be required to define the responsibilities of individuals, including outsourced staff, who have privileged access to the networks.

The cybersecurity policy of brokers trading through Application Programming Interface (APIs) based terminal should consider the principles prescribed by National Critical Information Infrastructure Protection Centre.

No person should have any intrinsic right to access confidential data by virtue of their rank or position. SEBI has asked brokers and depository participants to formulate a comprehensive cybersecurity and cyber resilience policy document encompassing the framework. The policy document should be approved by the board or proprietor of the broker and depository participants. In case of deviations from the suggested framework, reasons for such deviations, technical or otherwise, should be provided in the policy document. In case applications are offered to customers over the Internet by Market Infrastructure Institutions (MIIs) such as NSE's NOW and BSE's BEST among others, the responsibility of ensuring cyber resilience on those applications reside with the MIIs and not with the broker or depository participant. The cybersecurity policy of brokers trading through Application Programming Interface (APIs) based terminal should consider the principles prescribed by National Critical Information Infrastructure Protection Centre.

RBI to Tokenise Debit, Credit and Prepaid Transactions

Source: https://www.indiatoday.in

The 16-digit token will keep changing with every single transaction, making it impossible for any vendor or third-party to know actual debit or credit card number.

The Reserve Bank of India (RBI) has taken a major step to tokenise debit, credit and prepaid transactions in order to make such service more secure. Tokenisation involves a process in which a unique token, issued by the bank, masks sensitive card details. Thereafter, in lieu of actual card details, this token is used to perform card transactions. Instead of 16-digit card number, a randomly generated token ID issued by the bank, will be used. The 16-digit token will keep changing with every single transaction, making it impossible for any vendor or third-party to know actual debit or credit card number. Customers shopping online will only provide the generated token number in lieu of the actual card number. RBI, however, has made it clear that Additional Factor of Authentication (AFA)/ PIN entry shall be applicable for tokenised card transactions too. The card payment networks have been asked to employ a mechanism for periodic system audit at frequent intervals. A copy of this audit report shall be furnished to the Reserve Bank, with comments of auditors on deviations, said the top bank.

A Crisis Management Plan to Counter Cyber-attacks

Source: http://www.newsonair.com

The crisis management plan will be implemented by all Ministries and Departments of the Centre and the state governments in critical sectors.

Government of India has formulated a Crisis Management Plan to counter cyber-attacks and cyber terrorism. It will be implemented by all Ministries and Departments of the Centre and the state governments in critical sectors. Giving this information in a written reply, IT Minister Sh. Ravi Shankar Prasad told the Lok Sabha that the Government has empanelled 76 security audit organisations to ensure information security.

News Snippets - International

Global DNS Hijacking Campaign

Source: https://www.fireeye.com, https://www.cyberscoop.com

Global Cyber Security Firm FireEye identified a wave of DNS hijacking that affected dozens of domains belonging to government, telecommunications and Internet infrastructure entities across the Middle East, North Africa, Europe and North America. This campaign has targeted victims across the globe on an almost unprecedented scale, with a high degree of success. The attackers use this technique for their initial foothold, which can then be exploited in a variety of ways. Preliminary technical evidence assesses with moderate confidence that this activity is conducted by persons based in Iran. The United States Department of Homeland Security issued a rare "emergency" directive ordering federal civilian agencies to secure the login credentials for their Internet domain records. The emergency directive, which carries more urgency than DHS's more-common Binding Operational Directives, requires agencies to add multi-factor authentication to their DNS accounts, change account passwords, audit their DNS records, and monitor certificate logs, according to the order. Agencies had 10 business days to implement those instructions.

The United States Department of Homeland Security issued a rare "emergency" directive ordering federal civilian agencies to secure the login credentials for their Internet domain records.

Australia's Political Parties Suffered Cyber-attacks

Source: https://www.smh.com.au/

Australia's political parties suffered cyber-attacks alongside the Parliament House computer network by a "sophisticated state actor". Australian Prime Minister, Mr. Scott Morrison told Parliament that while investigating the parliamentary hack, cybersecurity authorities "also became aware that the networks of some political parties, Liberal, Labor and Nationals, have also been affected". "Our cyber experts believe that a sophisticated state actor is responsible for this malicious activity." Mr Morrison said the government had "put in place a number of measures to ensure the integrity of our electoral system". "I have instructed the Australian Cyber Security Centre to be ready to provide any political party or electoral body in Australia with immediate support, including making their technical experts available," he said. "They have already briefed the electoral commissions and those responsible for cyber security for all states and territories. They have also worked with global anti-virus companies to ensure Australia's friends and allies have the capacity to detect this malicious activity. We have acted decisively to protect our national interests."

The computer servers of Australia's major political parties have been hit by a cyber-attack with a "sophisticated state actor" suspected to be behind the plot, says the prime minister.

"Our cyber experts believe that a sophisticated state actor is responsible for this malicious activity."

Bank of Valletta Shut Down After Hackers Broke into its Systems

Source: https://www.timesofmalta.com

Hackers sought to make international transfers to banks in the UK, US, Czech Republic and Hong Kong.

Bank of Valletta, a Maltese bank shut down all its operations for a day after hackers broke into its systems and moved €13 million into foreign accounts. All of the bank's functions - branches, ATMs, mobile banking and even email services - were suspended and its website taken offline. The fraudulent transactions had been traced and were "being reversed", Prime Minister Joseph Muscat told parliament later. The attack is believed to have originated overseas. In a statement, the bank reassured customers that their accounts and funds "are in no way impacted or compromised". The attack was detected shortly after the start of business on Wednesday morning, Prime Minister Joseph Muscat told parliament, when it noted reconciliation problems regarding international transfers. Hackers sought to make international transfers to banks in the UK, US, Czech Republic and Hong Kong. The transfers were blocked within 30 minutes and the banks alerted, the Prime Minister said. There was some chaos in certain bigger shops, such as supermarkets, where they relied on the electronic devices for the majority of their payments.

DNC Email Addresses Targeted in a Spear-phishing Campaign

Source: https://www.theregister.co.uk

"It is probable that Cozy Bear again attempted to unlawfully infiltrate DNC computers in November 2018,"

Hackers attempted to infiltrate the Democratic National Committee (DNC) just after the US midterm elections last year, according to a new court filing. "On November 14, 2018, dozens of DNC email addresses were targeted in a spear-phishing campaign, although there is no evidence that the attack was successful," an amended complaint, filed in New York, states. The hacking effort has previously been connected to a Russian hacking group known as Cozy Bear. "It is probable that Cozy Bear again attempted to unlawfully infiltrate DNC computers in November 2018," the filing reports.

Cybercriminals Targeting Banks in Western African Nations

Source: http://www.scmagazine.com

Symantec said the attacks have been taking place since mid-2017 hitting financial institutions in Cameroon, Congo (DR), Ghana, Equatorial Guinea and Ivory Coast.

In a somewhat unusual step cybercriminals are targeting banks in several western African nations using off the shelf malware to gain entry, gain persistence and exfiltrate data along with "living off the land" tactics. Symantec said the attacks have been taking place since mid-2017 hitting financial institutions in Cameroon, Congo (DR), Ghana, Equatorial Guinea and Ivory Coast. The company noted attacking banks in these nations is somewhat outside the norm for cybercriminals, but noted expanding attacks into this region is likely another sign of the globalization of cybercrime.

A New Global Campaign Targeting Critical Sectors

Source: https://securingtomorrow.mcafee.com/

McAfee discovered a new global campaign targeting nuclear, defence, energy, and financial companies. This campaign, Operation Sharpshooter, leverages an in-memory implant to download and retrieve a second-stage implant called Rising Sun for further exploitation. The Rising Sun implant uses source code from the Lazarus Group's 2015 backdoor Trojan Duuzer in a new framework to infiltrate these key industries. This campaign, while masquerading as legitimate industry job recruitment activity, gathers information to monitor for potential exploitation. In October and November 2018, the Rising Sun implant has appeared in 87 organizations across the globe, predominantly in the United States. Most of the targeted organizations are English speaking or have an English-speaking regional office. According to report, the campaign is suspected to affect the Military/Telecommunication sector of India.

This campaign, while masquerading as legitimate industry job recruitment activity, gathers information to monitor for potential exploitation.

Trends

SS7 Exploit Intercepts the SMS sent for Two-factor-authentication

Source: http://www.scmagazine.com, https://motherboard.vice.com

In a recent attack, United Kingdom's (UK) Metro Bank became victim of Signalling System 7 (SS7) protocol exploit. Cyber-criminals are exploiting flaws in this protocol which is normally being used by telecom companies to coordinate routing of texts and calls around the world. Using this exploit, one can track phones across the world and can intercept phone calls, text messages without hacking the phone itself. According to UK National Cyber Security Centre, this exploit is also used to intercept codes used for banking. Hackers need to obtain their targets' online banking username and password and when banks ask for confirmation code sent via text message, the SS7 exploit intercepts the message sent for two-factor-authentication (2FA) and gains access to the account. The exploitation relies on the fact that SS7 network does not authenticate the sender of the request. To prevent this, an authenticator app or time-based one-time password (TOTP) can be used for 2FA.

Using this exploit, one can track phones across the world and can intercept phone calls, text messages without hacking the phone itself.

Blockchain of Etherium Classic was under Attack

Source: https://www.technologyreview.com

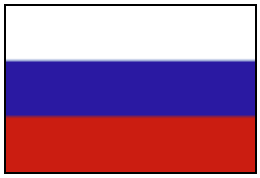
According to Coinbase, a popular cryptocurrency exchange platform, the blockchain of Etherium Classic cryptocurrency, was under attack. An attacker gained access to more than half of the network's computing power to rewrite the transaction history.

It made possible to spend the same currency more than once.

It made possible to spend the same currency more than once. Attacker was able to pull off around $1.1 million; however Coinbase claimed that no currency was actually stolen from any of its accounts. Blockchains are particularly attractive to thieves because fraudulent transactions can't be reversed as they often can be in the traditional financial system. The protocol isn't the only thing that has to be secure. To trade cryptocurrency, one has to run a software client, which can also contain vulnerabilities.

Russia is considering taking a Break from Global Internet Briefly

Source: https://www.bbc.com



A draft law called the Digital Economy National Program has been outlined which requires Russia's Internet Service Providers to operate in the event of foreign powers acting to isolate Russia online.

Following the Democratic Republic of Congo's decision to turn off Internet during presidential election, Russia is now considering to take a break from global Internet briefly as a test of its cyber-defence. This will lead to data between Russian citizens and organizations being not shared outside the nation. A draft law called the Digital Economy National Program has been outlined which requires Russia's Internet Service Providers to operate in the event of foreign powers acting to isolate Russia online. Russia may need to build their own version of Domain Name Server (DNS), as 12 organizations overseeing the root servers for DNS are none in Russia. The test is also expected to involve ISPs demonstrating that they can direct data to government-controlled routing points. These will filter traffic so that data sent between Russians reaches its destination, but any destined for foreign computers is discarded. The Russian government is providing cash for ISPs to modify their infrastructure so the redirection effort can be properly tested.

USA Legislation on Global Electoral Exchange Program

Source: https://www.nextgov.com

This Global Electoral Exchange Program would assist allies in adopting best practices around election.

Under Sens. Amy Klobuchar, D-Minn., and Dan Sullivan, R-Alaska, USA has reintroduced a legislation which would create a program at State to share information about election threats with other countries. This is in wake of misinformation campaigns and cyberattacks which threatens to undermine democracy around the world. This Global Electoral Exchange Program would assist allies in adopting best practices around election. It will also allow the agency to support non-profit groups that are involved in efforts to support international election integrity. It would award grants to groups that bring foreign election officials and polling workers to the U.S. to study election procedures. It would also open up funds to send U.S. officials to study the election processes of other democratic countries. A report on the program's activities will be presented every two years.

Guidelines on Cyber Security on-board Ships

Source: https://www.zdnet.com

A conglomerate of 21 international shipping associations and industry groups has released the third edition of the "Guidelines on Cyber Security on-board Ships". This report comes in the wake of recent cyber-attacks carried out by hackers. Electronic Chart Display and Information System (ECDIS) which ships use for sailing can be infected by viruses which results in delay in sailing for several days. Ransomware and improper RDP passwords can also compromise a ship's normal function. USB devices which are used to update systems or transfer new documents into air-gapped networks need to be handled carefully. Even due to improper security controls, some systems are left exposed online which are indexed by Shodan or Censys. There can be backdoor accounts in IT systems designed for ships. This document comes against the backdrop of Maersk, which was the biggest cargo shipping company in the world and was infected with the NotPetya ransomware. It incurred costs of over $300 million for recovery process.

Image Source: marineinsight.com
Image Credits: Sohit Shukla

Electronic Chart Display and Information System (ECDIS) which ships use for sailing can be infected by viruses which results in delay in sailing for several days.

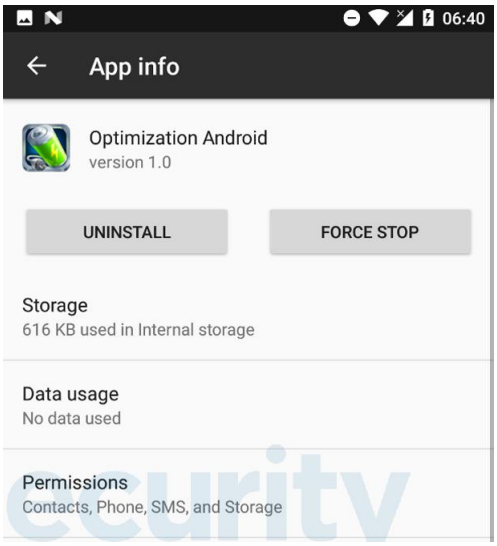
Cyber Campaign Directed at Intergovernmental Organizations

Source: https://cdn.area1security.com/

Beginning in April of 2015, Area 1 Security began observing technical artefacts of a cyber campaign directed at Intergovernmental Organizations, Ministries of Foreign Affairs and Ministries of Finance, as well as trade unions and think tanks. In late November 2018, Area 1 Security discovered that this campaign, via phishing, successfully gained access into the computer network of the Ministry of Foreign Affairs of Cyprus, a communications network used by the European Union to facilitate cooperation on foreign policy matters. This network, known as COREU, operates between the 28 EU countries, the Council of the European Union, the European External Action Service, and the European Commission. It is a crucial instrument in the EU system of foreign policymaking. The campaign was directed by the Chinese government and specifically undertaken by the Strategic Support Force (SSF) of the People's Liberation Army (PLA). While the targets are disparate, there is a consistent set of characteristics and chain of events that tie together a larger campaign that includes targeting the United Nations and the AFL-CIO in addition to accessing diplomatic cables from the COREU network.

This campaign, via phishing, successfully gained access into the computer network of the Ministry of Foreign Affairs of Cyprus

Malware Bytes

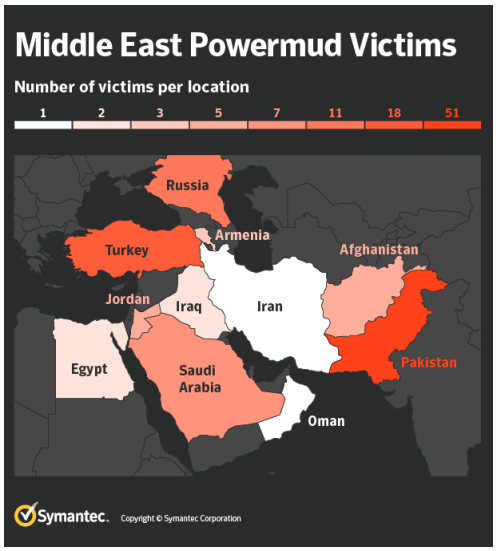


After being launched, the malicious app terminates without offering any functionality and hides its icon.

Android Malware Masquerading as Battery Optimization Tool

Source: https://www.welivesecurity.com

Trojans targeting Android users is not new. This new breed of malware is masquerading as a battery optimization tool, and is distributed via third-party app stores. After being launched, the malicious app terminates without offering any functionality and hides its icon. The malware's first function, stealing money from its victims' PayPal accounts, requires the activation of a malicious Accessibility service. This request is presented to the user as being from the "Enable statistics" service. Once the user opens the PayPal app and logs in, the malicious accessibility service (if previously enabled by the user) steps in and mimics the user's clicks to send money to the attacker's PayPal address. The malware's second function utilizes phishing screens covertly displayed over targeted, legitimate apps. By default, the malware downloads HTML-based overlay screens for five apps – Google Play, WhatsApp, Skype, Viber, and Gmail. Four of the five overlay screens phish for credit card details; the one targeting Gmail is after Gmail login credentials. The only way to get past this overlay screen is to fill out the bogus form.



The telecommunications and IT services sectors were the main targets.

Cyber-attacks Targeting the Middle East, Europe and America

Source: https://www.symantec.com/

Symantec uncovered extensive insights into a cyber espionage group behind a recent series of cyber-attacks designed to gather intelligence on targets spread primarily across the Middle East as well as in Europe and North America. The group, called Seedworm, has been operating since at least 2017, with its most recent activity observed in December 2018. In September 2018, Seedworm was found on a computer within the Brazil-based embassy of an oil-producing nation. Seedworm's motivations are to acquire actionable information about the targeted organizations and individuals. The Seedworm group controls its Powermud backdoor from behind a proxy network to hide the ultimate command-and-control location. After compromising a system, Seedworm first runs a tool that steals passwords saved in users' web browsers and email, demonstrating that access to the victim's email, social media, and chat accounts is one of their likely goals. Seedworm then uses open-source tools such as LaZagne and Crackmapexec to obtain Windows authorization credentials. Observed Seedworm victims were located primarily in Pakistan and Turkey, but also in Russia, Saudi Arabia, Afghanistan, Jordan, and elsewhere. Additionally, the group compromised organizations in Europe and North America that have ties to the Middle East. The Telecommunications and IT services sectors were the main targets.

A Campaign to Deliver Lures Pertaining to the Korean Region

Source: https://unit42.paloaltonetworks.com

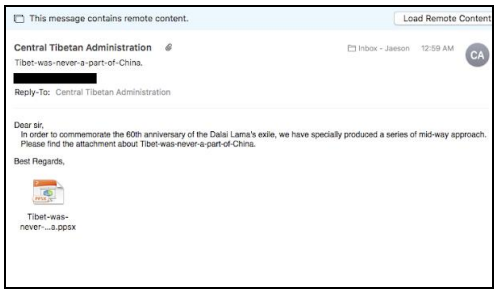
Unit 42 has uncovered a campaign that is being used to deliver lures primarily pertaining to the South Korea and North Korea region. These lures revolve around a series of subjects, including various cryptocurrencies, cryptocurrency exchanges, and political events. Unit 42 has dubbed this malware family CARROTBAT. CARROTBAT was initially discovered in an attack on December 2017. This attack was made against a British government agency using the SYSCON malware family. On December 13, 2017, a spear phishing email was sent from the email address of yuri.sidorav@yandex[.]ru to a high ranking individual within a British government agency. This email contained the subject "US. would talk with North Korea "without precondition"", with an attached document file of the same name.

These lures revolve around a series of subjects, including various cryptocurrencies, cryptocurrency exchanges, and political events.

A Malware Campaign Targeting Central Tibetan Administration

Source: https://blog.talosintelligence.com

Cisco Talos observed a malware campaign delivering a malicious Microsoft PowerPoint document using a mailing list run by the Central Tibetan Administration (CTA), an organization officially representing the Tibetan government-in-exile. The document used in the attack was a PPSX file, a file format used to deliver a non-editable slideshow derived from a Microsoft PowerPoint document. Given the nature of this malware and the targets involved, it is likely designed for espionage purposes rather than financial gain. The infrastructure used for the command and control in this campaign has been previously linked to the LuckyCat Android- and Windows-based trojans. Everyone on the CTA's mailing list received this email. The mailing list's infrastructure is run out of DearMail, an Indian company providing cloud enabled web-based email campaign manager. The attackers modified the standard Reply-To header normally used by the CTA mailings so that any responses would be directed back to an email address belonging to the attackers: mediabureauin [at] gmail.com. The email message itself references the upcoming 60th anniversary of the Dalai Lama's exile on March 31. The document is a large slide show, over 240 slides in length, claimed to have been created by the Central Tibetan Administration. This PPSX is a copy of a legitimate PDF available for download from the tibet.net homepage from the Central Tibetan Administration.



The PPSX document sent to the CTA mailing list

This PPSX is a copy of a legitimate PDF available for download from the tibet.net homepage from the Central Tibetan Administration.

Malicious Activities by DarkHydruns

Source: https://ti.360.net/

The mode of initial infection is via phishing mail by luring the victim to open the document. Once the document is opened, victim is asked to enable the macro

Activities have been observed about a targeted attack group named DarkHydruns. The mode of initial infection is via phishing mail by luring the victim to open the document. Once the document is opened, victim is asked to enable the macro which in turn drops a file 12-B-366.txt at location C:\TEMP which further drops the PowerShell script at Location %TEMP%\\WINDOWSTEMP.ps1. This PowerShell script drops the backdoor named as Officeupdateservice.exe on victim machine at location, %TEMP%\\OfficeUpdateService.exe. Backdoor has the capability of detecting Sandbox detection, sending collected information to Command and control (C2) server through Domain Name Server (DNS) tunnel to remain undetected for longer duration. Backdoor also maintain its persistence in victim machine and collect the host name information of victim system. Finally connect with C2 through DNS Tunnelling and, attacker send commands into victim machine for performing malicious activity like Upload content on C2, download script, DNS Record setting etc.

Shamoon Reappears with Doubly Destructive Component

Source: https://www.darkreading.com

Saipam, a leading provider of drilling services, described the attack as impacting up to 100 PCs and between 300 and 400 servers located in the Middle East, India, Scotland, and Italy.

Organizations in the United Arab Emirates and Saudi Arabia are targeted in a new wave of attacks involving Shamoon, a malware strain that was used to destroy more than 30,000 PCs at oil giant Saudi Aramco in 2012. The latest attacks come after a two-year lull and are doubly destructive since they include a new component, Filerase, for erasing files on an infected system before Shamoon wipes the master boot record clean. The addition of Filerase makes it almost impossible for victims to recover data from impacted systems. Based on a breach disclosure from Italian oil services firm Saipam, the new Shamoon attacks appear to have begun Dec. 10. Saipam, a leading provider of drilling services, described the attack as impacting up to 100 PCs and between 300 and 400 servers located in the Middle East, India, Scotland, and Italy. Reuters quoted a Saipem executive as saying the attacks had originated in the south Indian city of Chennai. However, Symantec have found evidence of attacks against at least two other organizations in the oil and gas industry in the Middle East during the same time. Once Filerase infects one system, it spreads across the victim network using a list of targeted systems and another tool called Spreader.exe. The list, in the form of a text file, is specific to each victim and suggests that the attackers likely gathered the information from previous reconnaissance activity on the network. Once Filerase has been successfully copied on all computers in the attacker's list, the Spreader component simultaneously triggers it on the systems.

ASUS Computers Targeted in a Massive Supply Chain Attack

Source: www.forbes.com, www.digit.in, www.dailymail.co.uk

About a million ASUS computers have been targeted in a massive supply chain attack dubbed "ShadowHammer", which leverages the ASUS Live Update software. ASUS Live Update is pre-installed on most ASUS computers and is used to automatically update certain components such as BIOS, UEFI, drivers and applications. According to cybersecurity firm Kaspersky, ASUS was used to unwittingly install a malicious backdoor on thousands of its customers' computers after attackers compromised a server for the company's live software update tool. The malware searched for targeted systems through their unique MAC addresses, if it found one of these targeted addresses, the malware reached out to a command-and-control server the attackers operated, and installed additional malware on those machines. Also the malicious file was signed with legitimate ASUS digital certificates to make it appear to be an authentic software update from the company. Asus released a statement saying that it had upgraded its software to prevent any malicious manipulation in the form of software updates or other means.


ASUS response to the recent media reports regarding ASUS Live Update tool attack by Advanced Persistent Threat (APT) groups

2019/03/27

ASUS response to the recent media reports regarding ASUS Live Update tool attack by Advanced Persistent Threat (APT) groups

Advanced Persistent Threat (APT) attacks are national-level attacks usually initiated by a couple of specific countries, targeting certain international organizations or entities instead of consumers.

ASUS Live Update is a proprietary tool supplied with ASUS notebook computers to ensure that the system always benefits from the latest drivers and firmware from ASUS. A small number of devices have been implanted with malicious code through a sophisticated attack on our Live Update servers in an attempt to target a very small and specific user group. ASUS customer service has been reaching out to affected users and providing assistance to ensure that the security risks are removed.

ASUS has also implemented a fix in the latest version (ver. 3.6.8) of the Live Update software, introduced multiple security verification mechanisms to prevent any malicious manipulation in the form of software updates or other means, and implemented an enhanced end-to-end encryption mechanism. At the same time, we have also updated and strengthened our server-to-end-user software architecture to prevent similar attacks from happening in the future.

ASUS statement published on its website

> *ASUS was used to unwittingly install a malicious backdoor on thousands of its customers' computers after attackers compromised a server for the company's live software update tool.*

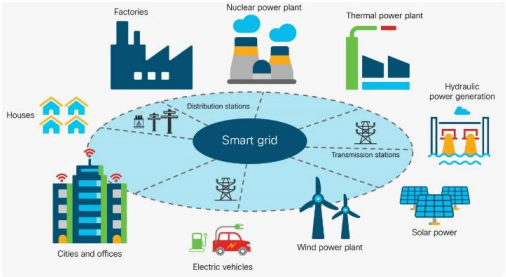
Learning

IoT Analytics for Electric Utilities

Sh. Ganesh Sahu, NCIIPC

Advances in technology now enable virtually anything to be connected to the Internet. This Internet of Things (IoT) represents one of the most profound technology innovations in history. We are in the midst of a transformative time when simply enormous numbers of devices are being connected to the global network. It is this exponential increase in connections that transforms the IoT into the Internet of Everything (IoE), creating both significant challenges and unprecedented opportunities for organizations around the world. Today's electric utilities are increasingly focused on grid modernization. Steadily increasing demand, integration of new sources of electricity in the form of wind and solar power, and the need to dynamically balance supply and demand are all driving the industry to embrace a fully connected world fuelled by real-time insight from data generated and analysed throughout the grid—from out at the edge of the network to the inner core of the enterprise data centre. Analytics powered by IoT-generated data enables utility companies to:

- Edge-driven analytics enable organizations to move from scheduled maintenance models to predictive ones, giving them dynamic control over their equipment and maintenance resources.



High level view of electrical grid (Image Source: cisco.com)

> *We are in the midst of a transformative time when simply enormous numbers of devices are being connected to the global network.*

- Integrate renewable resources more efficiently onto the grid with edge algorithms
- Provide more accurate insight on power quality; restore power faster after an outage by optimizing resources that minimize the duration of customer interruptions and increase restoration efficiency.
- Create personalized energy services for each customer, becoming the company of choice, not just for power but also for other home services

Know your supply chain, and be aware of vulnerabilities in IoT devices produced by third-party vendors outside of your organization

Recommendations

- Incorporate Security at the Design Phase - Avoid rushing new devices to market quickly without considering security vulnerabilities.
- Advanced Security Updates and Vulnerability Management - Flaws discovered after product deployment need to be continuously corrected with patching updates.
- Build on Proven Security Practices - Apply proven and tested security practices used successfully in traditional IT and network applications.
- Prioritize Security Measures According to Potential Impact - Focus on potential disruption consequences for each individual IoT application to prioritize security measures.
- Promote Transparency across IoT - Know your supply chain, and be aware of vulnerabilities in IoT devices produced by third-party vendors outside of your organization.
- Connect carefully and deliberately - Carefully consider whether continuous connectivity is needed.

References

[1] https://www.techmedics.com/2017/11/iot-security-awareness-security-recommendations-office/

[2] https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/big-data/solution-overview-c22-740248.pdf

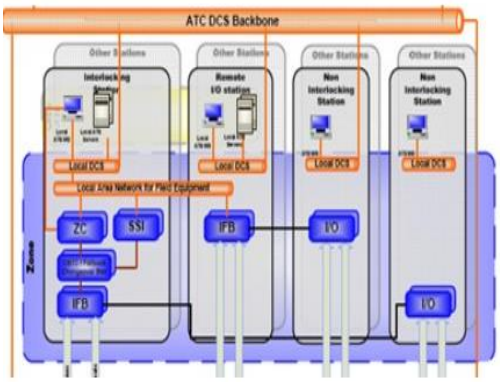
Cyber Security in Rail Metro system

Sh. Abhijeet Raj Shrivastava and Sh. Chandramohn K, NCIIPC

Urban Metro Railway systems are increasingly relying on Information and Communications Technologies (ICT). As metro transport is undergoing digital transformation, and industry becomes more dependent upon it. This evolution makes cybersecurity an important concern, in addition to the traditional focus on reliability, availability, maintainability and safety.

Communication Based Train Control (CBTC) and the European Rail Traffic Management Systems (ERTMS) are dominant radio-controlled systems are leading to a new era of rail transit control, enhancing flexibility, reducing maintenance costs and improving interoperability. A CBTC system is a continuous, automatic train control system utilizing high-resolution train location determination, independent from track circuits, continuous, high-capacity, bidirectional data communications and train borne and capable of implementing Automatic Train Protection (ATP) functions, as well as optional Automatic Train Operation (ATO) and Automatic Train Supervision (ATS) functions. This system consists of train borne systems, wayside systems, and a central management system, which are all connected continuously through high-speed data communication networks. CBTC makes use of RF-based data communication systems (DCSs) for train control and traffic management. CBTC systems have generally used IEEE 802.11wireless local area network (WLAN), widely known as Wi-Fi, as the radio technology, mainly due to its cost-effectiveness. Wi-Fi based on IEEE 802.11 standard is often selected in safety related applications like Vehicle-to-Vehicle (V2V) and Vehicle-to-Everything (V2X) in CBTC. Also CBTC employs European Train Control System (ETCS) radios to get the exact train position and then implement accurate vehicle positioning close passengers' platforms. These accelerated industry efforts in the deployment of CBTC systems have increased the level of risk that the public may potentially be exposed to as a result of the greater use of wireless technology. The most significant source of risk in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders as wireless networks have included not only traditional telecommunications systems, but also Industrial Control Systems (ICS)/ Supervisory control and data acquisition (SCADA) systems.

A CBTC system is a continuous, automatic train control system utilizing high-resolution train location determination, independent from track circuits, continuous, high-capacity, bidirectional data communications and train borne and capable of implementing Automa tic Train Protection functions



Automatic Train Control system & Data Communication System

CBTC System Vulnerability Attacks

Active attacks: An adversary on-board the train with laptop can perform various attacks against the intra-vehicular Wi-Fi communication. More sophisticated forms of active attack are the Denial of Service (DOS) or the more advanced Distributed Denial of Service (DDOS).

Passive attacks: Passive attack is a result of the secretive way information is gathered. It is the easiest type of attack to execute, and the hardest to defend against. This kind of attack is particularly easy due to not enabling confidential features of wireless technology or the numerous vulnerabilities in the wireless system.

Securing CBTC in the Digital and Communication Environment

- Confidentiality is concerned with ensuring that the data and systems are not to be disclosed to unauthorized individuals.
- User authentication methods range from time invariant weak authentication methods such as simple passwords to time variant strong cryptographically based authentication methods.
- Use of WiMAX and LTE as a secondary link to the private wireless network and use of Cloud Computing.
- Providing regular security health check by providing risk assessment Monitoring and patching of the systems.

References

[1] https://www.mobility.siemens.com/mobility/global

[2] https://cgc.al-enterprise.co.id/wp-content/uploads/2017/06/Protecting-rail-and-metro-from-cyber-security-threats-FINAL-VERSION1

[3] https://www.smartrailworld.com/cybercrime-and-terrorism-the-growing-twin-threats-to-rail-and-metro

[4] http://www.irse.org/knowledge/publicdocuments

[5] https://www.witpress.com/Secure/elibrary/papers/CR06/CR06068FU1.pdf

User authentication methods range from time invariant weak authentication methods such as simple passwords to time variant strong cryptographically based authentication methods.

Web Application Firewall

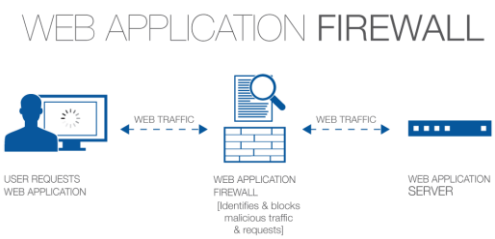
Sh. Arun Sharma, NCIIPC

A Web Application Firewall (WAF) filters, monitors, and blocks HTTP traffic to and from a Web application. A WAF is an application firewall for HTTP applications, which applies a set of rules to an HTTP conversation. It protects against Layer 7 attacks. A WAF can either network-based, host-based or cloud based and is often deployed through a proxy and is placed in front of one or more Web applications. WAF is an application firewall for HTTP applications, which applies a set of rules to an HTTP conversation. Usually, these rules cover common attacks like Cross-site Scripting (XSS) and SQL injection etc. WAF proactively protects websites and applications against fraud or data theft; blocking any suspicious activity. A WAF can be considered as a reverse proxy; a proxy that retrieves resources on behalf of client from one or more servers. [1]

WAF for Protection of Critical Web Applications

Organisations rely increasingly on Web applications to run their business. Web attackers are also an Organisation's greatest threat.

WAF proactively protects websites and applications against fraud or data theft; blocking any suspicious activity.



Hackers are becoming more aggressive – continually devising smarter ways to gain unauthorized access to Web applications. Web attacks affect business of all sizes, and can result in data breaches on a massive scale. Whether it's to access data, steal assets or cause disruption, the impact on enterprise operations, business continuity, and company reputation can be catastrophic. WAF provides robust defence against sophisticated and targeted attacks. WAF makes it easy to manage consistent security policies for all Web applications, from a single source. On filtering and monitoring HTTP(s) traffic to and from Web applications, WAF makes it easier to mitigate enterprise risk and minimise vulnerabilities, especially against inbound and complex targeted attacks. According to the Open Web Application Security Project (OWASP), WAF applies set of rules to an HTTP conversation to block common attacks. Therefore, a WAF is designed to patch application weaknesses. [2]

WAF makes it easier to mitigate enterprise risk and minimise vulnerabilities, especially against inbound and complex targeted attacks.

Key Considerations in Choosing WAF

Today, Organisations are extending their business by using more Web-based and Cloud-hosted applications, so a robust and agile WAF is no more a luxury – it's a bare essential requirement. Since, Web applications are migrating to cloud-based Infrastructure-as-a-Service (IaaS) environment and Organisations are leveraging on Cloud Software-as-a-Service (SaaS) applications, security teams are borne to be challenged to protect Web applications at no cost of compromising on performance, scalability & manageability. Therefore, the following basic consideration should be considered when selecting a WAF:

Network Architecture & Application Infrastructure: In this inline model, the three methods can be used to pass the traffic: Reverse-proxy mode, Router mode and Bridge mode. The best deployment option must be opted which understands scope of services one should need to use.

Virtual Patching & Scanner Integration: Virtual patches are key component of strong WAF, usually requires integration with vulnerability scanner. Make sure to pick a WAF solution that seamlessly integrates with class leading scanner technologies.

Automatic Attack Detection: A strong WAF extends bot-defence capabilities to deliver always-on protection – preventing automated 7 DDoS attacks, Web scraping and brute force Attacks. At minimum a WAF today should be able to detect attacks, designed to respond challenges. [3]

On deploying a strong Web application firewall, one can secure their Critical Web applications. A powerful WAF solution enables organisations to protect against application vulnerabilities, zero-day attacks and OWASP top 10 threats.

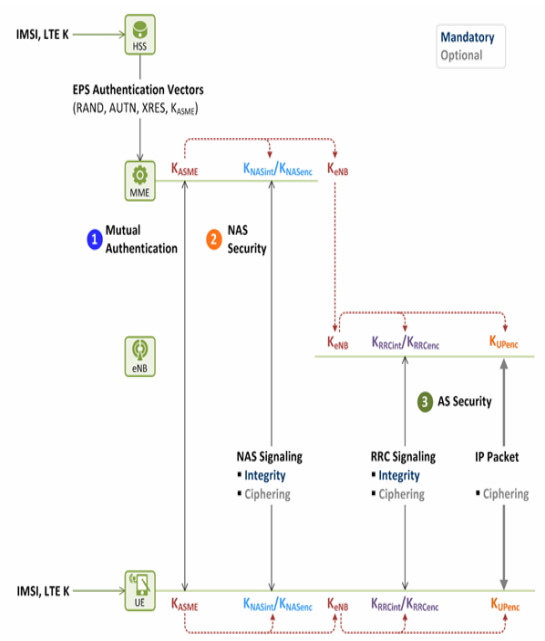
A good WAF also enables compliance with key standards like HIPAA and PCI DSS. [3]

References

[1] Wikipedia – The free encyclopaedia

[2] https://www.tatacommunications.com/wp-content/uploads/2018/10/cloud-web-application-firewall-email-4.pdf

[3] https://www.f5.com/services/resources/white- papers/key-considerations-in-choosing-a-web-application-firewall



Cyber Security in LTE (4G) Telecom Network

Sh. Neeraj Saini, NCIIPC

LTE end-to-end security involves the following elements:

Authentication and Key Agreement (AKA): The foundation of LTE security is authenticating the UEs (User Equipment's) and wireless networks. This can be accomplished using the AKA process which asserts that the serving network authenticates the identity of a user and the UE certifies the network signature. The AKA creates encryption and integrity keys applied for originating various session keys for ensuring the 4G/LTE security and privacy.

Confidentiality and Integrity of signalling security of network access control planes is achieved when the RCC (Rescue Coordination Centre) and NAS (Non-Access Stratum) layer signalling is encrypted and integrity protected. Ciphering and integrity protection of LTE RRC (Radio Resource Control) signalling is executed at the packet data convergence protocol (PDCP) layer, whereas the NAS layer attains the protection by encrypting the NAS-level signalling. This protection cannot be uniquely performed for each UE connection, but it runs across trusted connections between AGW (Application Gate Way) and eNodeB (Evolve Node B).

User plane confidentiality LTE has a security feature for user plane via encrypting data/voice between the UE and eNodeB. Encryption is executed at the IP layer by utilizing IPsec-based tunnels between AGW and eNodeB, but no integrity protection is offered for the user plane due to performance and efficiency considerations. The PDCP layer is used for enabling encrypting/decrypting the user plane while transmitting traffic between the eNodeB and UE.

References

[1] https://www.statista.com/ statistics/206615/

[2] www.netmanias.com

[3] www.nmcgroups.com

Three Strategies for Delivering a Comprehensive DDoS Defence

Source: https://www.fifthdomain.com

Distributed Denial-of-Service (DDoS) attack remains among the most destructive cyber challenges facing military, enterprise and public network infrastructure. To survive, organizations need network and information systems whose designs are fundamentally more resilient to DDoS, not just patches and filters to blunt the attacks. Innovative and adaptive strategies to confuse, confound and outwit attackers can be both more effective and less costly. Three strategies for delivering a comprehensive DDoS defence include:

Disperse high-value network assets: DDoS attackers target systems' most valuable information assets, centralized servers that include email, chat, login or DNS servers that are valuable sources of data. One tactic to combat this is to decentralize or disperse the log data or DNS IP information an adversary wants to target. This will make it more difficult for attackers to target data assets and minimize the impact of attacks.

Deceptive defence: One the best ways to defend against a predator is to trick them. Through game-theory planning, real-time analytics and sophisticated network manoeuvring, adversary attack activity can be tracked, and appropriate counter manoeuvres can be implemented. For instance, an attacker could be fooled into thinking their attack is successful when it's not.

Sensor-driven response: Organizations need an adaptive DDoS capability to identify and mitigate attacks, especially zero-day precision attacks that happen in real time which exhaust targeted servers' computing capacity. With high fidelity sensors, organizations can quickly detect potential malicious activity, send an alert that will trigger an investigation and initiate appropriate mitigation responses.

One the best ways to defend against a predator is to trick them. Through game-theory planning, real-time analytics and sophisticated network manoeuvring, adversary attack activity can be tracked, and appropriate counter manoeuvres can be implemented.

The First 24 Hours of the Incident

Source: https://www.informationsecuritybuzz.com

In the early phases of a cybersecurity incident senior management typically want a clear understanding of what damage has been done, if any sensitive data has been stolen and how the attacker gained access. The responsibility to track down the route cause and contain the incident typically lies with the Computer Emergency Response Team (CERT)/Incident Response (IR) practitioners. To ensure this process can be carried out effectively adopting a triage process in the first 24 hours of the incident can provide a head-start in the remediation and post-incident investigation attempts.

Adopting a triage process in the first 24 hours of the incident can provide a head-start in the remediation and post-incident investigation attempts

Detection: Understanding how and when the incident was first detected is the ideal place to begin the timeline. Asking questions such as whether firewall logs are being used to their full potential to identify the initial compromise or if there are other Security Information and Event Management (SIEM) solutions in place could help to uncover vital clues.

System Framework: In order to provide an effective response knowing where the servers and endpoints are physically located is important. Equally important is the setup, i.e. operating systems, storage, virtualisation as well as security configuration, i.e. user groups/permissions as well as a network map.

To ensure that IT, CISO and IR single point of contacts (SPoC) are fully engaged with one another it is essential that this communication is continued throughout the course of the incident response plan.

Preliminary Remediation: Providing accurate handover notes to the IR team along with a record of the steps taken up until that point to be recommended in order to prevent any cross-contamination or incorrect leads being pursued. To ensure that IT, CISO and IR single point of contacts (SPoC) are fully engaged with one another it is essential that this communication is continued throughout the course of the incident response plan.

Logs: Log files may be crucial in identifying Indicators of Compromise (IoC). To avoid mislaying any evidence logging must be fully enabled and retention periods applied and provided at the earliest opportunity to determine IoCs.

Artefact Preservation: The preservation of artefacts identified within data must be maintained to carry out comprehensive forensic analysis and so that an accurate timeline can be constructed.

Each incident must be treated on an individual basis and this process should be employed whether or not external authorities are engaged.

Vulnerability Watch

Critical Vulnerability in FreeBSD

Source: https://www.freebsd.org/

Insufficient bounds checking vulnerability (CVE-2018-17160) has been discovered in one of the device models provided by bhyve(8) that can permit a guest operating system to overwrite memory in the bhyve(8) processing possibly permitting arbitrary code executions. A guest OS using a firmware image can cause the bhyve process to crash, or possibly execute arbitrary code on the host as root. Versions before 11.2-STABLE (r341486) and 11.2-RELEASE-p6 are vulnerable. It has a CVSS 3.0 Base Score of 10.0. Users are advised to upgrade the vulnerable system with the patch released.

Multiple Vulnerabilities in VyOS

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

A sandbox escape issue (CVE-2018-18555) and privilege escalation issue (CVE-2018-18556) was discovered in VyOS 1.1.8. It has a CVSS 3.0 Base Score of 9.9. Sandbox escape issue provides a restricted management shell for operator users to administer the device. By issuing various shell special characters with certain commands, an authenticated operator user can break out of the management shell and gain access to the underlying Linux shell. The user can then run arbitrary operating system commands with the privileges afforded by their account. Privilege escalation issue allows operator users to execute the pppd binary with elevated (sudo) permissions. Certain input parameters are not properly validated. A malicious operator user can run the binary with elevated permissions and leverage its improper input validation condition to spawn an attacker-controlled shell with root privileges.

Critical Vulnerability in Kubernetes

Source: https://nvd.nist.gov/vuln/detail/CVE-2018-18843

The GitLab Kubernetes integration is vulnerable to a Server-Side Request Forgery (SSRF) issue (CVE-2018-18843) which could allow an attacker to make requests to access any internal URLs. GitLab Enterprise Edition 11.x before 11.2.8, 11.3.x before 11.3.9, and 11.4.x before 11.4.4 are vulnerable. It has a CVSS 3.0 Base Score of 10.0. The issue is now mitigated in the latest release.

Critical Vulnerability in TIM 1531 IRC

Source: https://cert-portal.siemens.com

TIM 1531 IRC is a communication module for SIMATIC S7-1500, S7-400, S7-300 with SINAUT ST7 with three RJ45 interfaces for communication via IP-based networks (WAN / LAN) and a RS-232/RS-485- interface for communication via classic WAN networks. The device was missing proper authentication (CVE-2018-13816) when connecting on port 102/tcp, although configured. An attacker needs to be able to connect to port 102/tcp of an affected device in order to exploit this vulnerability. The vulnerability could allow an attacker to perform administrative operations. It has a CVSS 3.0 Base Score of 10.0. Siemens has released updates for TIM 1531 IRC modules.

An attacker needs to be able to connect to port 102/tcp of an affected device in order to exploit this vulnerability

Critical Vulnerability in MicroMathematics

Source: https://nvd.nist.gov/vuln/detail/CVE-2018-1000821

XML External Entity (XXE) vulnerability has been found in MicroMathematics (CVE-2018-1000821).

This affects function of the component SMathStudio File Handler.

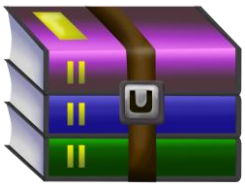
This affects function of the component *SMathStudio File Handler*. Version before commit 5c05ac8 contains vulnerability in SMathStudio files that can result in Disclosure of confidential data, denial of service, SSRF, port scanning. It has a CVSS 3.0 Base Score of 10.0. This vulnerability has been fixed in after commit 5c05ac8.

This vulnerability affects the functionality of the component GSA XML File Parser.

Critical Vulnerability in CodeLibs Fess

Source: https://nvd.nist.gov/vuln/detail/CVE-2018-1000822

XML External Entity (XXE) vulnerability (CVE-2018-1000822) was found in codelibs fess. This vulnerability affects the functionality of the component *GSA XML File Parser*. Codelibs fess version before commit faa265b contains the vulnerability in GSA XML file parser that can result in Disclosure of confidential data, denial of service, SSRF, port scanning. This attack appears to be exploitable via specially crafted GSA XML files. This vulnerability appears to have been fixed in after commit faa265b. It has a CVSS 3.0 Base Score of 10.0.

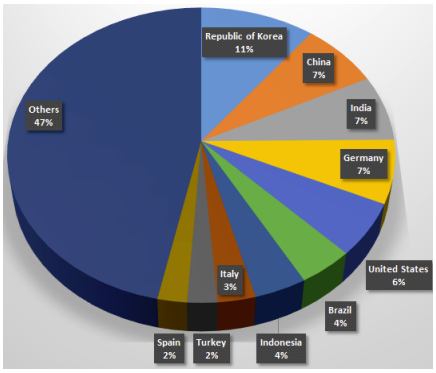


WinRAR itself does not contain auto-update features, increasing the likelihood that many existing users running out-of-date versions

WinRAR Zero-day Abused in Multiple Campaigns

Source: https://www.fireeye.com

Path traversal zero-day vulnerability (CVE-2018-20250) has been found in WinRAR that enables attackers to specify arbitrary destinations during file extraction of 'ACE' formatted files, regardless of user input. Attackers can achieve persistence and code execution by creating malicious archives that extract files to sensitive locations. Multiple campaigns such as Impersonating an Educational Accreditation Council etc. leveraging this vulnerability have been observed. This vulnerability has been fixed in the latest version of WinRAR (5.70). However, WinRAR itself does not contain auto-update features, increasing the likelihood that many existing users running out-of-date versions.



Successful decryptions per country

Security App

Decryption Tool for Systems Infected with GandCrab

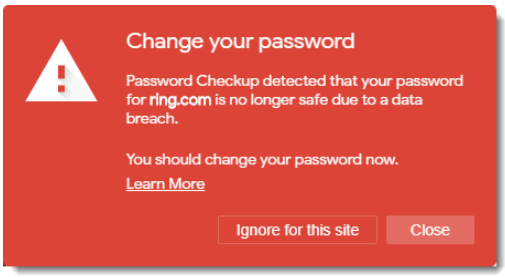
Source: https://labs.bitdefender.com

Bitdefender Labs has released the new version of their GandCrab decryptor. GandCrab has inflicted hundreds of millions of dollars in losses globally since its emergence, and is now one of the most prevalent families of ransomware on the market. Bitdefender Labs provides this decryption tool for free and anybody can download and decrypt their systems infected with GandCrab Ransomware.

"Since our first decryptor, in aggregate we have already helped nearly 20,000 victims save a minimum of $18 million US dollars by the end of February" says Bitdefender Labs.

Chrome Extension for Checking Passwords Exposed in Breach

Source: https://chrome.google.com/



A new Chrome Extension from Google called "Password Checkup" will automatically check whether the user passwords have been exposed in a data breach. Once installed, the extension checks any login details against a database of around four billion usernames and passwords, and warns if it finds a match. "Password checkup" sends confidential login information to Google for verifying against the database but Google says in description of this extension: "Password Checkup was built with privacy in mind. It never reports any identifying information about your accounts, passwords, or device."

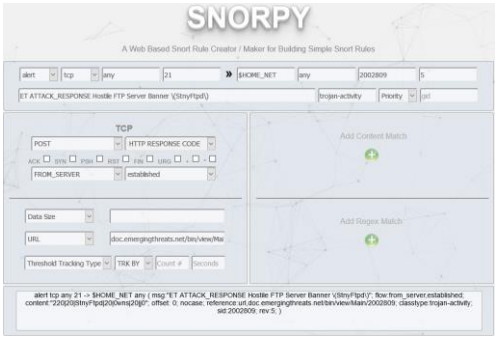
URLhaus – Website with list of Malware URLs

https://urlhaus.abuse.ch/about/

URLhaus is a project operated by abuse.ch. This site collects, tracks and shares malware URLs, which helps network administrators and security analysts to protect their network. URLhaus provides data for both, commercial and non-commercial purpose without any limitation. It even has customized delivery mechanism other than APIs.

Snorpy – An Application to Build Custom Snort/Suricata Rules

Source: https://isc.sans.edu/



Snorpy is a web base application to easily build Snort/Suricata rules in a graphical way. Building Rules for Snort and Suricata in a command line is very complicated and tedious and one must be well versed with syntax of the rules. This tool will come very handy for the security analysts to create their own custom Snort and Suricata rules. It is simple to use starting from the Action and Protocol fields and as you pick each field, the rule builder shows the rule in the bottom window

ReiKey – macOS Tool to Alert of Key Loggers

https://objective-see.com/products/reikey.html

Malware and other applications may install persistent keyboard "event taps" to intercept user keystrokes. ReiKey can scan, detect, and monitor for such taps.

ReiKey has two main capabilities: scanning for existing keyboard "event taps", and alerting whenever a new keyboard event tap is activated.

ReiKey is designed to detect such keyboard taps, alerting the user anytime a new tap is installed. In other words its goal is to detect the most common type of macOS keyloggers. ReiKey has two main capabilities: scanning for existing keyboard "event taps", and alerting whenever a new keyboard event tap is activated.

NCIIPC Initiatives

Workshop at Punjab Police Academy

NCIIPC, in collaboration with Punjab Police organised a one day information security sensitisation workshop on Critical Information Infrastructure Protection at Punjab Police Academy, Phillaur on 18th January 2019. The workshop was attended by 38 officials of Punjab Police. Sh. Abhijeet Raj Shrivastava and Sh. Rakesh Kumar from NCIIPC delivered talks during the workshop.

Sh. Rakesh Kumar, Sectoral Coordinator (Govt.), NCIIPC delivering talk in workshop

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:

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

- Sh. Adesh Nandkishor Kolte
- Sh. Shivam Singh
- Sh. Arif Khan
- Sh. Saurabh Pandey
- Sh. Subhamoy Guha
- Sh. Antriksh Shah
- Sh. Tushar Shinde
- Ms. Anjali Patil
- Sh. Akash Sharma
- Sh. Remesh Ramachandran
- Sh. Nikhil Suthar
- Sh. Sangram Jagdale
- Ms Namrata Arvikar
- Sh. Raju Kumar
- Sh. Rahul
- Ms. Sushma Ahuja
- Sh. Shreyas Thakare
- Sh. Chetan Tiwari
- Sh. Himanshu Rahi
- Sh. Saurabh SIngh

- Ms. Salunkhe Khushbu
- Sh. Uday Ahire (Vick Nick)
- Sh. Aniruddha Khadse
- Sh. Mayank
- Sh. Sreekanth Pillai
- Sh. Mukesh Kumar Rao
- Sh. Mitesh Patil
- Sh. Ketan Madhukar Mukane
- Sh. Lavanya Srivastava
- Sh. Sreedeep.ck Alavil
- Sh. Ninad Mishra
- Sh. Brijesh Singh, IPS
- Sh. Punit Darji
- Sh. Dipak Prajapati
- Sh. Lav Kumar Vishwakarma
- Sh. Sumit Lakra

International Conference on Cybersecurity and Data Protection

NCIIPC participated in 1st International Conference on "Cybersecurity and Data Protection – Regulatory Compliance for India" held on 15th Mar 2019 at New Delhi. The conference was focused on best global practices, policy and regulations, covering Cybersecurity for Critical Infrastructure, European Union General Data Protection Regulation, Indian Data Protection and Privacy Bill and Future state of Internet of Things. Col Pradeep Bhat (Retd), Consultant NCIIPC moderated a session on Cyber Security for Critical Infrastructure. Gp Capt R K Singh and Sh Abhijeet Raj Shrivastava from NCIIPC took part in the conference.

Col Pradeep Bhat (Retd) from NCIIPC moderated a session on Cyber Security for Critical Infrastructure

NCIIPC at India Smart Utility Week 2019

India Smart Utility Week (ISUW) 2019 was organized as an International Conference and Exhibition on Smart Energy and Water for Smarter Cities from 12-16 March 2019 in New Delhi. ISUW 2019 brought together India's leading Electricity, Gas and Water Utilities, Policy Makers, Regulators, Investors and world's top-notch Smart Energy Experts and Researchers to discuss trends, share best practices and showcase next generation technologies and products in smart energy and smart cities domains. ISUW 2019 included plenaries, interactive workshops, keynotes, and technical sessions. Dr. Ajeet Bajpai, Director General, NCIIPC delivered talk on 'Securing the CII in Power Sector' and some associated concerns as part of Panel Discussion on 'Cyber Secure Energy Transition and Utility Transformation: Resiliency and Future Readiness'.

Dr. Ajeet Bajpai, Director General, NCIIPC delivered talk on importance of CII declaration and its protection for the power sector utilities

Sh. H.S. Dhillon, ADG NCIIPC delivered the keynote address on TechSummit Industry 4.0

NCIIPC as Cyber Security Partner for TechKriti 2019

NCIIPC participated as Cyber Security Partner in annual technical festival of Indian Institute of Technology, Kanpur (IITK). TechKriti is the Asia's largest technical and entrepreneurial fest organized by the students of IIT Kanpur. Its 25th edition was held on 7-10 March 2019 at IITK. Sh. H.S. Dhillon, ADG NCIIPC delivered the keynote address on TechSummit Industry 4.0. He elaborated on cyber security issues in the coming days for next industrial revolution. The event had around 40000 footfalls from 1000 colleges. Various events like Capture the Flag, Code Golf etc. were organised in association with NCIIPC.

Defend the Flag: Cooperative Banking Cyber Security Edition

NCIIPC organized a two-day event "DTF: Cooperative Banking Cyber Security Edition" on 27-28 Feb 2019 at Mumbai. Defend The Flag (DTF) event was organised in collaboration with Information Sharing and Analysis Centre (ISAC) and Tata Communications Ltd. The event brought together the top decision makers from each sector to discuss the latest developments in cyber security, issues/challenges faced by companies and most importantly learn from each other the best practices in Cyber Security that would greatly enhance the overall resilience of cyber space across India.

One Day Information Sensitisation Workshop for States and UTs

NCIIPC organised a one day information security sensitisation workshop for States and Union Territories on 14th December 2018. The event was attended by the officials from various states looking after the critical information infrastructure. The event was aimed to cover emerging Cyber Security Threats, Challenges and Mitigation Strategies.

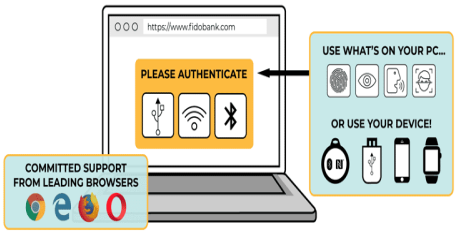
NCIIPC Delivered Keynote Talk at BRICS Conference

Sh Ganesh Kumar Sahu, Sectoral Coordinator (Power & Energy), NCIIPC delivered keynote talk on Critical Infrastructure Security at Building Resilient India in Cyber Space (BRICS) conference on 21 Feb 2019 organised by Veermata Jijabai Technological Institute (VJTI) Mumbai. The conference was focused on the current trends, need and future requirements of innovation in the field of cybersecurity for a secured cyber space. The workshop brought speakers from all the stakeholders like Industry, Academia, Government and Non-Profit organizations working in this space to brainstorm on current challenges and future aspects which need to be addressed for resilient, robust and secure cyberspace.

Mobile Security

FIDO2 Certification Rolled Out for Android 7 Nougat and Above

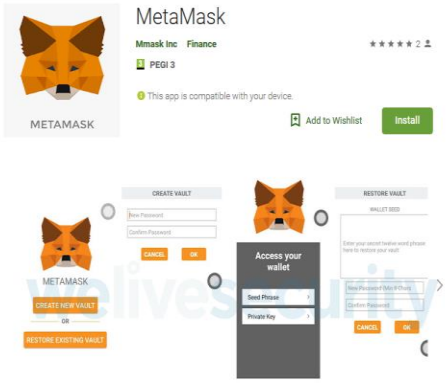
Source: https://thehackernews.com



By updating Google Play Services, Android Nougat 7 and above users can take advantage of FIDO2 (Fast Identity Online) protocol which offers password-less authentication through Android's authentication mechanisms like PIN or swipe pattern or built-in fingerprint sensor based on standard public key cryptography. This protocol is a combination of W3C's WebAuthn API which uses FIDO authentication into web browsers and FIDO's Client to Authenticator Protocol (CTAP). This works on all major browsers like Google Chrome, Microsoft Edge and Mozilla Firefox etc.

Android Clipper Malware Found on Play Store

Source: https://www.welivesecurity.com



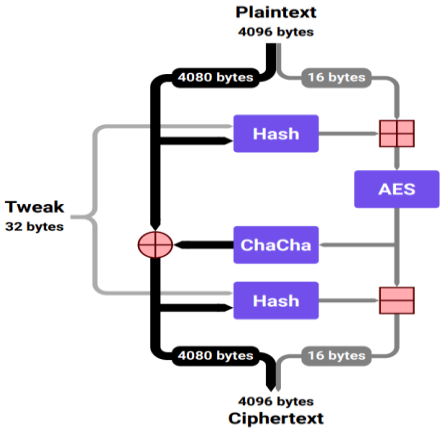
ESET researchers have discovered the first android Trojan clipper dubbed Android/Clipper.C whose purpose is to steal crypto currency and bit coin. Attackers have tricked users in installing a malicious app impersonating a legitimate crypto currency service "MetaMask". This "Clipper" malware then replaces the crypto currency wallet address made up of long strings of characters from the user's clipboard with the attacker's wallet address and thus redirects the payment to attacker's account. This malicious app was first spotted at app store on February 1, 2019 and now has already been taken down by Google.

DrainerBot: A Major Mobile Advertisement Fraud Operation

Source: https://www.oracle.com

Oracle technology teams from its Moat and Dyn acquisitions have uncovered a major mobile ad fraud operation called DrainerBot which is distributed through infected consumer apps and games, such as "Perfect365", "VertexClub", "Draw Clash of Clans", "Touch 'n' Beat - Cinema" and "Solitaire: 4 Seasons (Full)". These apps have been downloaded more than 10 million times. This app-based fraud operation uses infected code to deliver invisible video ads to Android devices and thus consumes significant bandwidth and battery. Consumption of more than 10GB data per month has been reported which leads to more data charges by device owner. Tapcore, a company in Netherlands has distributed the SDK being used in these apps.

This app-based fraud operation uses infected code to deliver invisible video ads to Android devices and thus consumes significant bandwidth and battery.



Adiantum Storage Encryption for Low-End Android Devices

Source: https://security.googleblog.com

Google has released Adiantum storage encryption for low-end processors due to poor support of AES via ARMv8 Cryptography Extensions. Adiantum allows use of ChaCha stream cipher in a length-preserving mode and adapts ideas from AES-based proposals for length-preserving encryption such as HCTR and HCH. On ARM Cortex-A7, Adiantum encryption and decryption on 4096-byte sectors is about 10.6 cycles per byte, around 5x faster than AES-256-XTS. It is also true wide-block mode.

Anubis Strikes Again

Source: https://blog.trendmicro.com

Trend Micro has recently discovered two android apps named "Currency Converter" and "BatterySaverMobi" which are banking malwares. These apps drop malicious payload known as Anubis (ANDROIDOS_ANUBISDROPPER) in the victim's device. It connects to a C&C server with the domain aserogeege.space and 18 other malicious domains mapped to the IP address 47.254.26.2. These apps use device's motions such as sensing user's steps to hide their activities. These apps try to trick the users into downloading and installing its payload APK with a fake system update. Anubis then steals users' account credentials using a built-in key logger. Currently, it has been distributed to 93 different countries with 377 variations of financial apps.

PNG Image Exploit Android Devices

Source: https://source.android.com/

A specially crafted PNG image can compromise an Android device having Nougat 7.0 or above. Three vulnerabilities touted as CVE-2019-1986, CVE-2019-1987 and CVE-2019-1988 has already been patched by Google in its February 2019 security update. The security updates revealed repairing of some bugs like "buffering overflow", "SkpPngCodec errors" etc. related to rendering of PNG format images. An attacker can send this crafted PNG using an instant messaging service or as an attachment in an email, or it can be downloaded from any web-page.

CVE	References	Type
CVE-2019-1986	A-117838472 [2]	RCE
CVE-2019-1987	A-118143775 [2]	RCE
CVE-2019-1988	A-118372692	RCE

Upcoming Events - Global

April 2019

- InfoSec World, Lake Buena Vista 1-3 Apr
- Financial Services Information Security Network, Windsor 8-9 Apr
- CSO50 Conference, Scottsdale 8-10 Apr
- SecureCISO New York, New York 11 Apr
- Cyber-Tech Women's Symposium, Pennsylvania 12 Apr
- Cybersecurity in Healthcare – How to Prevent the Next Attack, California 17 Apr
- 2019 Industrial Control Systems Cyber Security Conference, Singapore 16-18 Apr
- (ISC)² Secure Summit DC, Washington 23-24 Apr
- Ai4 Cybersecurity, New York 29-30 Apr

May 2019

- CyberCon IV, Des Moines 7-8 May
- Keep Watch: The Manufacturing Security Conference, Miami 9-10 May
- Airport Security & IT Summit, Barcelona 16-17 May
- Cyber Security Exchange Healthcare, Dallas 19-21 May
- IEEE Workshop on the Internet of Safe Things , San Francisco 20-22 May
- International Workshop on Traffic Measurements for Cybersecurity, San Francisco 23 May
- Global AppSec, Tel Aviv 26-30 May
- Artificial Intelligence in Financial Service Conference, Johannesburg 29-30 May
- CircleCityCon 6.0, Indianapolis 31 May-2 Jun

June 2019

- International Conference on Cyber Incident Response, Coordination, Containment & Control (Cyber Incident), Oxford 3-4 Jun
- International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford 3-4 Jun
- International Workshop on Cyber Insurance and Risk Controls (CIRC), Oxford 3-4 Jun
- C4ISRNET CONFERENCE, ARLINGTON 6 Jun
- Gartner Security and Risk Management Summit National Harbor 17-20 Jun
- International Workshop on Cyber Range Technologies and Applications, Stockholm 20 Jun
- Security Operations Summit & Training, New Orleans 21 Jun-1Jul

APRIL 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				

MAY 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	

JUNE 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						

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			

July 2019

- Security IT Summit, London 2 Jul
- 5th VDI Conference – Cyber Security for Vehicles, Dusseldorf 9-10 Jul
- The CybSec and Blockchain Health , London 11-12 Jul
- High Performance Mission Critical System Development, Dublin 15-19 Jul
- RSA Conference 2019, Singapore 16-18 Jul
- CISO Leadership Forum, Boston 24-25 Jul

Upcoming Events - India

- CII eMobility Summit, Pune 12 Apr
- India Internet Day, Gurgaon 25 Apr
- Gartner IT Infrastructure, Operations & Cloud Strategies Conference 2019, Mumbai 6 May
- IT-SA INDIA 2019 CONFERENCE, Mumbai 15-16 May
- Gartner Data & Analytics Summit, Mumbai 10-11Jun
- Nullcon Security Training, Bangalore 20-22 Jun
- International Cyber Security 3rd edition, Mumbai 21 Jun
- Cyber Security Conference, Avasa, Hyderabad 4-5 Sep
- Kenes Exhibitions Cyber Security Conference, Hyderabad 4-5 Sep
- HAKON – International Information Security Meet, Indore 13 Oct
- International Conference on Cyberlaw, Cybercrime & Cybersecurity, New Delhi 20-22 Nov

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

Feedback/Contribution

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

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.