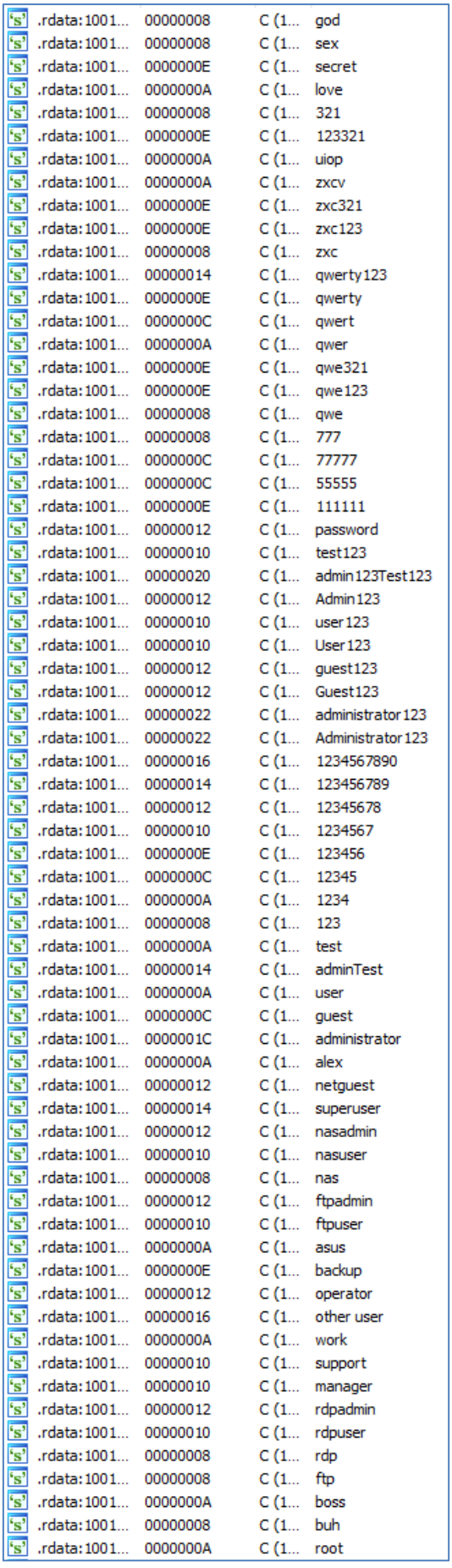
NCIIPC Alert on BadRabbit Ransomware

(27 October 2017)

NCIIPC alerts its stakeholders about the BadRabbit Ransomware hitting around the globe. Cisco Talos reports that a fake Flash Player update is being delivered. When users visited compromised websites, they were redirected to 1dnscontrol[.]com, the site which was hosting the malicious file. Before the actual malicious file was downloaded a HTTP POST request was observed to a static IP address (185.149.120[.]3). This request was found to be posting to a static path of "/scholasgoogle" and provided the user agent, referring site, cookie, and domain name of the session. After the POST the dropper was downloaded from two different paths from 1dnscontrol[.]com, /index.php and /flash_install.php. The malware appears to have been active for approximately six hours before the server 1dnscontrol[.]com was taken down. The initial download was observed around 24 Oct 2017 08:22 UTC.

The dropper (630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da) requires a user to facilitate the infection and does not use any exploit to compromise the system directly. This dropper contains the BadRabbit ransomware. Once installed there is an SMB component used for lateral movement and further infection. This appears to use a combination of an included list of weak credentials and a version of mimikatz similar to that which was used in Nyetya. Below is a list of the username/password combinations that are observed. This exploit takes advantage of a vulnerability described in the Microsoft MS17-010 security bulletin.



's'	.rdata:1001...	00000008	C (1...	god
's'	.rdata:1001...	00000008	C (1...	sex
's'	.rdata:1001...	0000000E	C (1...	secret
's'	.rdata:1001...	0000000A	C (1...	love
's'	.rdata:1001...	00000008	C (1...	321
's'	.rdata:1001...	0000000E	C (1...	123321
's'	.rdata:1001...	0000000A	C (1...	uiop
's'	.rdata:1001...	0000000A	C (1...	zxcv
's'	.rdata:1001...	0000000E	C (1...	zxc321
's'	.rdata:1001...	0000000E	C (1...	zxc123
's'	.rdata:1001...	00000008	C (1...	zxc
's'	.rdata:1001...	00000014	C (1...	qwerty123
's'	.rdata:1001...	0000000E	C (1...	qwerty
's'	.rdata:1001...	0000000C	C (1...	qwert
's'	.rdata:1001...	0000000A	C (1...	qwer
's'	.rdata:1001...	0000000E	C (1...	qwe321
's'	.rdata:1001...	0000000E	C (1...	qwe123
's'	.rdata:1001...	00000008	C (1...	qwe
's'	.rdata:1001...	00000008	C (1...	777
's'	.rdata:1001...	0000000C	C (1...	77777
's'	.rdata:1001...	0000000C	C (1...	55555
's'	.rdata:1001...	0000000E	C (1...	111111
's'	.rdata:1001...	00000012	C (1...	password
's'	.rdata:1001...	00000010	C (1...	test123
's'	.rdata:1001...	00000020	C (1...	admin123Test123
's'	.rdata:1001...	00000012	C (1...	Admin123
's'	.rdata:1001...	00000010	C (1...	user123
's'	.rdata:1001...	00000010	C (1...	User123
's'	.rdata:1001...	00000012	C (1...	guest123
's'	.rdata:1001...	00000012	C (1...	Guest123
's'	.rdata:1001...	00000022	C (1...	administrator123
's'	.rdata:1001...	00000022	C (1...	Administrator123
's'	.rdata:1001...	00000016	C (1...	1234567890
's'	.rdata:1001...	00000014	C (1...	123456789
's'	.rdata:1001...	00000012	C (1...	12345678
's'	.rdata:1001...	00000010	C (1...	1234567
's'	.rdata:1001...	0000000E	C (1...	123456
's'	.rdata:1001...	0000000C	C (1...	12345
's'	.rdata:1001...	0000000A	C (1...	1234
's'	.rdata:1001...	00000008	C (1...	123
's'	.rdata:1001...	0000000A	C (1...	test
's'	.rdata:1001...	00000014	C (1...	adminTest
's'	.rdata:1001...	0000000A	C (1...	user
's'	.rdata:1001...	0000000C	C (1...	guest
's'	.rdata:1001...	0000001C	C (1...	administrator
's'	.rdata:1001...	0000000A	C (1...	alex
's'	.rdata:1001...	00000012	C (1...	netguest
's'	.rdata:1001...	00000014	C (1...	superuser
's'	.rdata:1001...	00000012	C (1...	nasadmin
's'	.rdata:1001...	00000010	C (1...	nasuser
's'	.rdata:1001...	00000008	C (1...	nas
's'	.rdata:1001...	00000012	C (1...	ftpadmin
's'	.rdata:1001...	00000010	C (1...	ftpuser
's'	.rdata:1001...	0000000A	C (1...	asus
's'	.rdata:1001...	0000000E	C (1...	backup
's'	.rdata:1001...	00000012	C (1...	operator
's'	.rdata:1001...	00000016	C (1...	other user
's'	.rdata:1001...	0000000A	C (1...	work
's'	.rdata:1001...	00000010	C (1...	support
's'	.rdata:1001...	00000010	C (1...	manager
's'	.rdata:1001...	00000012	C (1...	rdpadmin
's'	.rdata:1001...	00000010	C (1...	rdpuser
's'	.rdata:1001...	00000008	C (1...	rdp
's'	.rdata:1001...	00000008	C (1...	ftp
's'	.rdata:1001...	0000000A	C (1...	boss
's'	.rdata:1001...	00000008	C (1...	buh
's'	.rdata:1001...	0000000A	C (1...	root

Indicators of Compromise:

Hashes (SHA256):

Dropper

- 630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da

Payload

- 8ebc97e05c8e1073bda2efb6f4d00ad7e789260afa2c276f0c72740b838a0a93 C:\Windows\dispci.exe (diskcryptor client)
- 682ADCB55FE4649F7B22505A54A9DBC454B4090FC2BB84AF7DB5B0908F3B7806 C:\Windows\cscc.dat (x32 diskcryptor drv)
- 0b2f863f4119dc88a22cc97c0a136c88a0127cb026751303b045f7322a8972f6 C:\Windows\cscc.dat (x64 diskcryptor drv)
- 579FD8A0385482FB4C789561A30B09F25671E86422F40EF5CCA2036B28F99648 C:\Windows\infpub.dat
- 2f8c54f9fa8e47596a3beff0031f85360e56840c77f71c6a573ace6f46412035 (mimikatz-like x86)
- 301b905eb98d8d6bb559c04bbda26628a942b2c4107c07a02e8f753bdcfe347c (mimikatz-like x64)

Scheduled Tasks names:

- viserion_
- rhaegal
- drogon

Domains:

Distribution Domain

- 1dnscontrol[.]com

Distribution Paths

- /flash_install.php
- /index.php

Intermediary Server

- 185.149.120[.]3

Referrer Sites:

- Argumentiru[.]com

- Fontanka[.]ru
- Adblibri[.]ro
- Spbvoditel[.]ru
- Grupovo[.]bg
- www.sinematurk[.]com

Hidden service:

- caforssztxqzf2nm[.]onion

Remediation: In this attack the user needs to facilitate the initial infection. If a user doesn't help the process along by installing the flash update it would be benign and not wreak the devastation it has across the region. Once a user facilitates the initial infection the malware leverages existing methods, such as SMB, to propagate around the network without user interaction.

Source: The above information has been taken from CISCO Threat Intelligence Feed http://blog.talosintelligence.com/2017/10/bad-rabbit.html

For further information please refer https://securelist.com/bad-rabbit-ransomware/82851/

Contact:

NCIIPC, Block III, Old JNU Campus, New Delhi-110067

Helpline: 1800-11-4430

Email: helpdesk1@nciipc.gov.in; helpdesk2@nciipc.gov.in