NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

August 2018, Edition 1.0

NETWORK INTELLIGENCE SECURITY ADVISORY

Everything you need to know about the latest threat components cropping up globally and also the remediation solutions to them.

IN THIS EDITION:

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

An active Campaigns Distributing FELIXROOT Backdoor

Severity: High
Date: July 30, 2018

IMPACT

An active campaign of Russian-Based threat actors, found distributing FelixRoot Backdoor through Word document embedded with malicious macros and taking advantage of known vulnerabilities (CVE-2017-11882 & CVE-2017-0199) to have persistent foothold on the compromised networks or systems.

REMEDIATION

- Ensure Microsoft Windows Workstations and Servers are up-to-date with the latest security patches.
- Ensure Antivirus Signature Database is up-to-date and Antivirus scan is run on daily or weekly basis.
- Ensure patch for Microsoft Office Memory Corruption Vulnerability (CVE-2017-11882), and Microsoft Office/WordPad Remote Code Execution Vulnerability (CVE-2017-0199) are applied on the Windows Workstations and Servers.
- Block IP/Hashes mentioned under Indicator of Compromise section, on security devices.

THREAT CAPABILITIES

Russian-Based threat actors are capable of maintaining persist foothold on the target network or system.

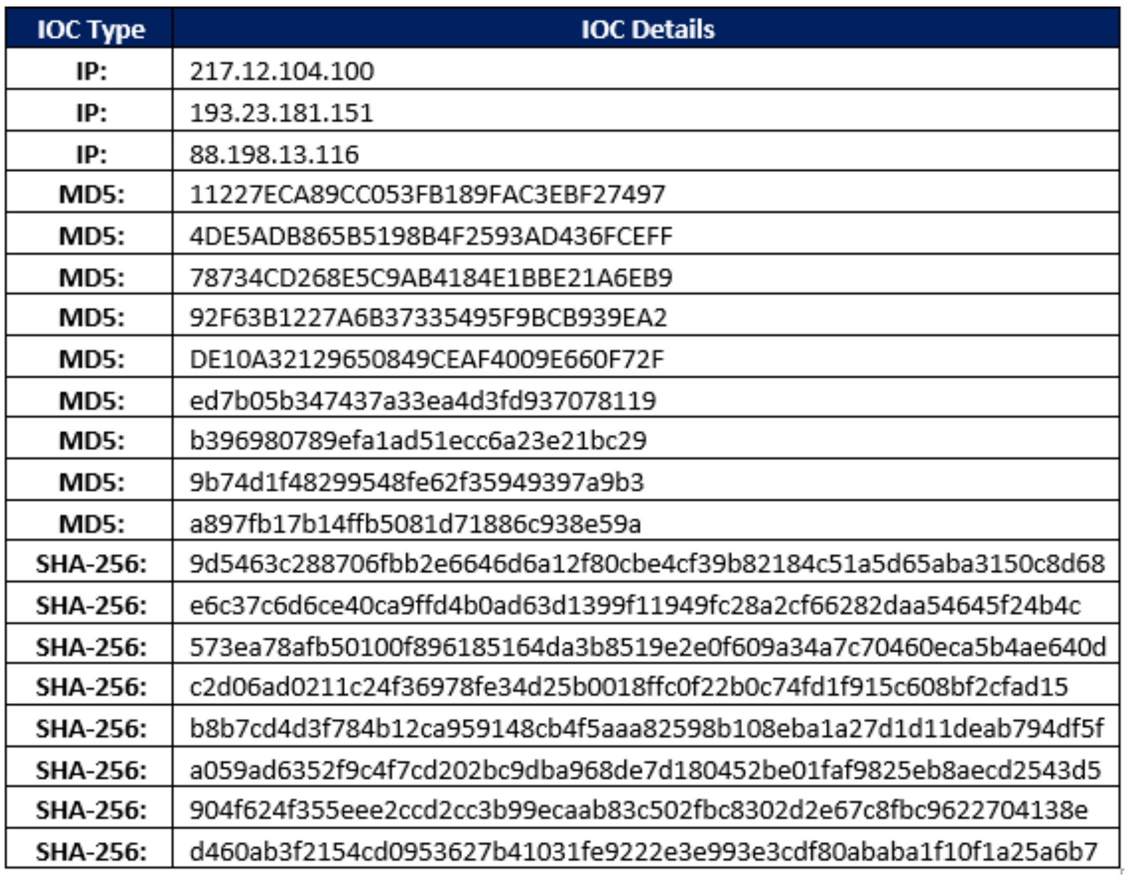
- The "FelixRoot" backdoor deployed by this threat actors will allow them to have lateral movement, network infiltration and data exfiltration on the target network or system.
- Additionally, it will allow them to scan for known vulnerabilities CVE-2017-11882 and CVE-2017-0199, during network infiltration on the target network.

READ

FELIXROOT Backdoor is back in a new fresh spam campaign

Microsoft Office Vulnerabilities Used to Distribute FELIXROOT Backdoor in Recent Campaign

INDICATORS OF COMPROMISE



IOC Type	IOC Details
IP:	217.12.104.100
IP:	193.23.181.151
IP:	88.198.13.116
MD5:	11227ECA89CC053FB189FAC3EBF27497
MD5:	4DE5ADB865B5198B4F2593AD436FCEFF
MD5:	78734CD268E5C9AB4184E1BBE21A6EB9
MD5:	92F63B1227A6B37335495F9BCB939EA2
MD5:	DE10A32129650849CEAF4009E660F72F
MD5:	ed7b05b347437a33ea4d3fd937078119
MD5:	b396980789efa1ad51ecc6a23e21bc29
MD5:	9b74d1f48299548fe62f35949397a9b3
MD5:	a897fb17b14ffb5081d71886c938e59a
SHA-256:	9d5463c288706fbb2e6646d6a12f80cbe4cf39b82184c51a5d65aba3150c8d68
SHA-256:	e6c37c6d6ce40ca9ffd4b0ad63d1399f11949fc28a2cf66282daa54645f24b4c
SHA-256:	573ea78afb50100f896185164da3b8519e2e0f609a34a7c70460eca5b4ae640d
SHA-256:	c2d06ad0211c24f36978fe34d25b0018ffc0f22b0c74fd1f915c608bf2cfad15
SHA-256:	b8b7cd4d3f784b12ca959148cb4f5aaa82598b108eba1a27d1d11deab794df5f
SHA-256:	a059ad6352f9c4f7cd202bc9dba968de7d180452be01faf9825eb8aecd2543d5
SHA-256:	904f624f355eee2ccd2cc3b99ecaab83c502fbc8302d2e67c8fbc9622704138e
SHA-256:	d460ab3f2154cd0953627b41031fe9222e3e993e3cdf80ababa1f10f1a25a6b7

Drupal affected by Security Bypass Vulnerability in Symfony, Zend Feed and Zend Diactoros libraries

Severity: Critical
Date: August 3, 2018

IMPACT

Drupal platform affected by Security Bypass Vulnerability (CVE-2018-14773) found in third-party libraries i.e., Symfony, Zend Feed and Zend Diactoros. This vulnerability would allow remote attacker to compromise web services.

REMEDIATION

- **For Drupal Platform**, Kindly upgrade to Drupal version 8.5.6.

For Symfony:

- If you're using Symfony 2.7.0 to 2.7.48, kindly update to latest version 2.7.49.
- If you're using Symfony 2.8.0 to 2.8.43, kindly update to latest version 2.8.44.
- If you're using Symfony 3.3.0 to 3.3.17, kindly update to latest version 3.3.18.
- If you're using Symfony 3.4.0 to 3.4.13, kindly update to latest version 3.4.14.
- If you're using Symfony 4.0.0 to 4.0.13, kindly update to latest version 4.0.14.
- If you're using Symfony 4.1.0 to 4.1.2, kindly update to latest version 4.1.3.

For Zend:

- Kindly update previous version of Zend-diactoros to version 1.8.4.
- Kindly update previous version of Zend-http to version 2.8.1.
- Kindly update previous version of Zend-feed to version 2.10.3.

VULNERABILITY

Following Drupal versions and third-party libraries are affected by this Security Bypass Vulnerability (CVE-2018-14773):

Drupal:
Drupal Platform prior to version 8.5.5, are affected.

Symfony:
Symfony 2.7.0 to 2.7.48, 2.8.0 to 2.8.43, 3.3.0 to 3.3.17, 3.4.0 to 3.4.13, 4.0.0 to 4.0.13 and 4.1.0 to 4.1.2 versions of the Symfony HttpFoundation component are affected.

Zend:
Zend-diactoros version earlier to version 1.8.4, are affected.
Zend-http version earlier to version 2.8.1, are affected.
Zend-feed version earlier to version 2.10.3, are affected.

Important Notice
Drupal:
Drupal platform prior to version 8.5.5 are end-of-life and do not receive security coverage.

Symfony:
The vulnerability has been fixed in Symfony 2.7.49, 2.8.44, 3.3.18, 3.4.14, 4.0.14, and 4.1.3.
No (vulnerability or bug) fixes are provided for Symfony 3.0, 3.1, and 3.2, as they are no longer supported.

Zend:
The vulnerability has been fixed in Zend-diactoros version 1.8.4.
The vulnerability has been fixed in Zend-http version 2.8.1.
The vulnerability has been fixed in Zend-feed version 2.10.3.

READ

Drupal Core - 3rd-party libraries -SA-CORE-2018-005 Drupal™

CVE-2018-14773: Remove support for legacy and risky HTTP headers Symfony

ZF2018-01: URL Rewrite vulnerability ZEND FRAMEWORK

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Parasite HTTP - A new Remote Access Trojan (RAT) uses advanced techniques to evade detection

Severity: High

Date: August 6, 2018

IMPACT

A new Remote Access Trojan (RAT) called Parasite HTTP found using advanced techniques to evade detection and remain persistent on the target network or system. It was first spotted on October 29, 2017, and underwent continuous development phase to add more functionalities. It was again spotted early this year on January 26, 2018, with newly added functionalities and was under product evaluation phase for two weeks before it was officially released on underground hacking forum. Since February 09, 2018, the RAT Parasite HTTP is being sold on underground hacking forum running under the shadow of Dark Web, with active support from malware author. This is a serious threat to the information and information system, which can cause data breach, breach of security controls and leaves no trace to conduct Incident Response.

REMEDIATION

- Ensure Microsoft Windows Workstations and Servers are up-to-date with the latest security patches.
- Ensure Antivirus Signature Database is up-to-date and Antivirus scan is run on daily or weekly basis.
- Block IP/Domain/Hashes mentioned under Indicator of Compromise section on security devices.

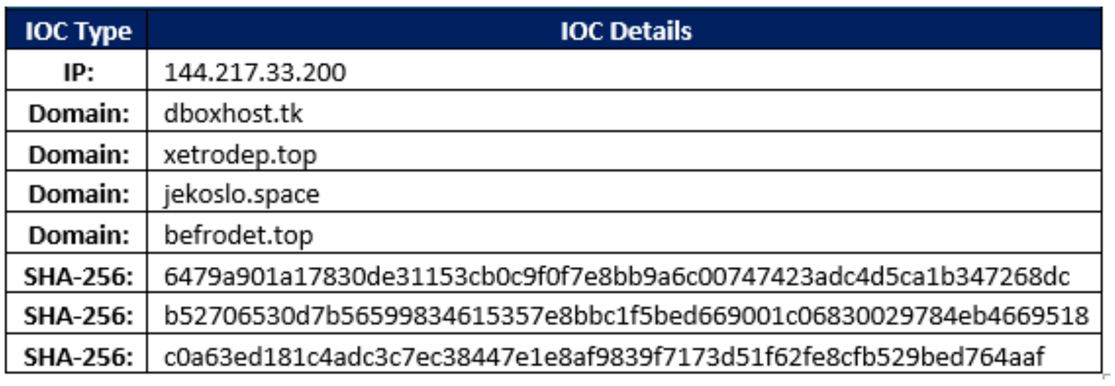
THREAT CAPABILITIES

- The RAT Parasite HTTP uses sandbox detection, anti-debugging, anti-emulation, and other protections techniques to evade detection.
- It is also modular in nature which allows the attacker to add new capabilities as they become available or download additional modules during post infection.
- It allows the attacker to have persisted foothold on the target network or system.

READ

- Highly Sophisticated Parasite RAT Emerges on the Dark Web threatpost
- Parasite HTTP RAT cooks up a stew of stealthy tricks proofpoint

INDICATORS OF COMPROMISE



IOC Type	IOC Details
IP:	144.217.33.200
Domain:	dboxhost.tk
Domain:	xetrodep.top
Domain:	jekoslo.space
Domain:	befrodet.top
SHA-256:	6479a901a17830de31153cb0c9f0f7e8bb9a6c00747423adc4d5ca1b347268dc
SHA-256:	b52706530d7b56599834615357e8bbc1f5bed669001c06830029784eb4669518
SHA-256:	c0a63ed181c4adc3c7ec38447e1e8af9839f7173d51f62fe8cfb529bed764aaf

New variant of AZORult malware campaign found distributing Hermes Ransomware

Severity: Critical

Date: August 6, 2018

IMPACT

A new variant of AZORult malware is active since July 16, 2018 and it is sold as a product on underground hacking forums. Ransomware as a new functionality has been added through update roll out on July 17, 2018 which have extended the scope of malware operations alongside information stealer & downloader. This new variant of AZORult malware now capable of distributing Hermes ransomware via large email campaign and drive-by-download methods, onto the target systems.

REMEDIATION

- Ensure Microsoft Windows Workstations and Servers are up-to-date with the latest security patches.
- Ensure Antivirus Signature Database is up-to-date and Antivirus scan is run on daily or weekly basis.
- Ensure Windows & Linux Operating Systems are running the latest version of Adobe Flash Player.
- Block IP/Domain/Hashes mentioned under Indicator of Compromise section below, on security devices.

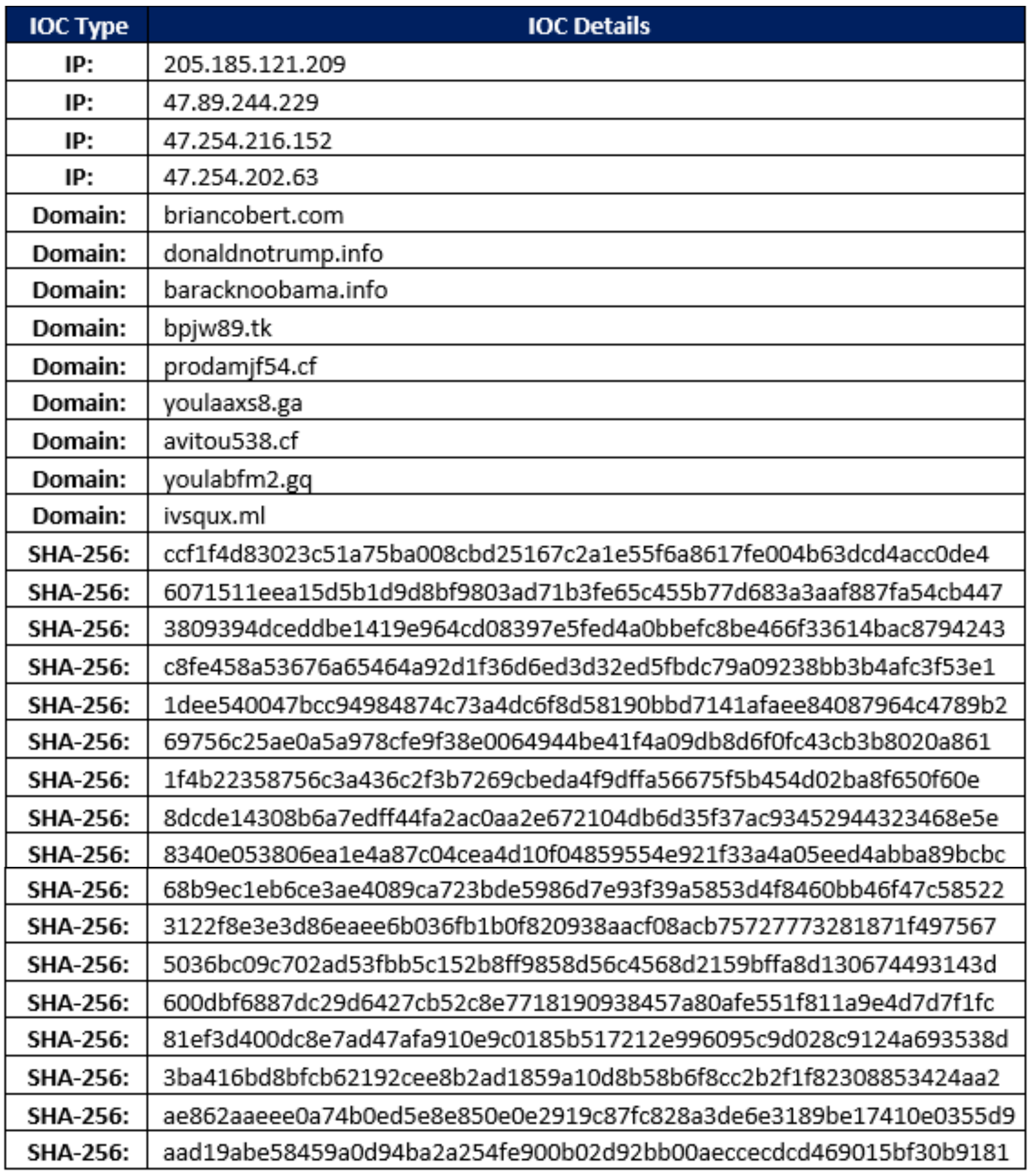
THREAT CAPABILITIES

- AZORult malware campaigns capable of sending thousands of spam messages to contact list of victim's Outlook address book.
- It is capable of stealing credential and cryptocurrency from the victim.
- It is also capable of causing data loss and disruption of business operations by performing Hermes ransomware attack alongside malware operation.

READ

- Updated AZORult info stealer/downloader used to spread ransomware shortly after appearing on dark web SC
- New version of AZORult stealer improves loading features, spreads alongside ransomware in new campaign proofpoint.

INDICATORS OF COMPROMISE



IOC Type	IOC Details
IP:	205.185.121.209
IP:	47.89.244.229
IP:	47.254.216.152
IP:	47.254.202.63
Domain:	briancobert.com
Domain:	donaldnotrump.info
Domain:	baracknoobama.info
Domain:	bpjw89.tk
Domain:	prodamjf54.cf
Domain:	youlaaxs8.ga
Domain:	avitou538.cf
Domain:	youlabfm2.gq
Domain:	ivsqux.ml
SHA-256:	ccf1f4d83023c51a75ba008cbd25167c2a1e55f6a8617fe004b63dcd4acc0de4
SHA-256:	6071511eea15d5b1d9d8bf9803ad71b3fe65c455b77d683a3aaf887fa54cb447
SHA-256:	3809394dceddbe1419e964cd08397e5fed4a0bbefc8be466f33614bac8794243
SHA-256:	c8fe458a53676a65464a92d1f36d6ed3d32ed5fbdc79a09238bb3b4afc3f53e1
SHA-256:	1dee540047bcc94984874c73a4dc6f8d58190bbd7141afaee84087964c4789b2
SHA-256:	69756c25ae0a5a978cfe9f38e0064944be41f4a09db8d6f0fc43cb3b8020a861
SHA-256:	1f4b22358756c3a436c2f3b7269cbeda4f9dffa56675f5b454d02ba8f650f60e
SHA-256:	8dcde14308b6a7edff44fa2ac0aa2e672104db6d35f37ac93452944323468e5e
SHA-256:	8340e053806ea1e4a87c04cea4d10f04859554e921f33a4a05eed4abba89bcbc
SHA-256:	68b9ec1eb6ce3ae4089ca723bde5986d7e93f39a5853d4f8460bb46f47c58522
SHA-256:	3122f8e3e3d86eaee6b036fb1b0f820938aacf08acb75727773281871f497567
SHA-256:	5036bc09c702ad53fbb5c152b8ff9858d56c4568d2159bffa8d130674493143d
SHA-256:	600dbf6887dc29d6427cb52c8e7718190938457a80afe551f811a9e4d7d7f1fc
SHA-256:	81ef3d400dc8e7ad47afa910e9c0185b517212e996095c9d028c9124a693538d
SHA-256:	3ba416bd8bfcb62192cee8b2ad1859a10d8b58b6f8cc2b2f1f82308853424aa2
SHA-256:	ae862aaeee0a74b0ed5e8e850e0e2919c87fc828a3de6e3189be17410e0355d9
SHA-256:	aad19abe58459a0d94ba2a254fe900b02d92bb00aeccecdcd469015bf30b9181

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

A mass phishing campaign distributing Shrug2 Ransomware

Severity: Critical
Date: August 10, 2018

IMPACT

New Shrug2 Ransomware found targeting Banks and financial institutions on a global scale. This Ransomware is built on .NET framework and has additional capabilities similar to Banking Trojan. This ransomware is distributed via phishing campaign and demands a ransom of $70 USD in the form of Bitcoin for decrypting files. This poses a serious risk of data loss, data breach, financial losses and can cause disruption in business operations.

REMEDIATION

- Ensure Microsoft Windows Workstations and Servers are up-to-date with the latest security patches.
- Ensure Antivirus Signature Database is up-to-date and Antivirus scan is run on daily or weekly basis.
- Block IP/Subnet/Domain/Hashes mentioned under Indicators of Compromise section below, on security devices.
- An active subscription to Anti-Phishing service and Security Awareness training is highly recommended to identify and eliminate the weak chain in Organization’s Cyber Defence.

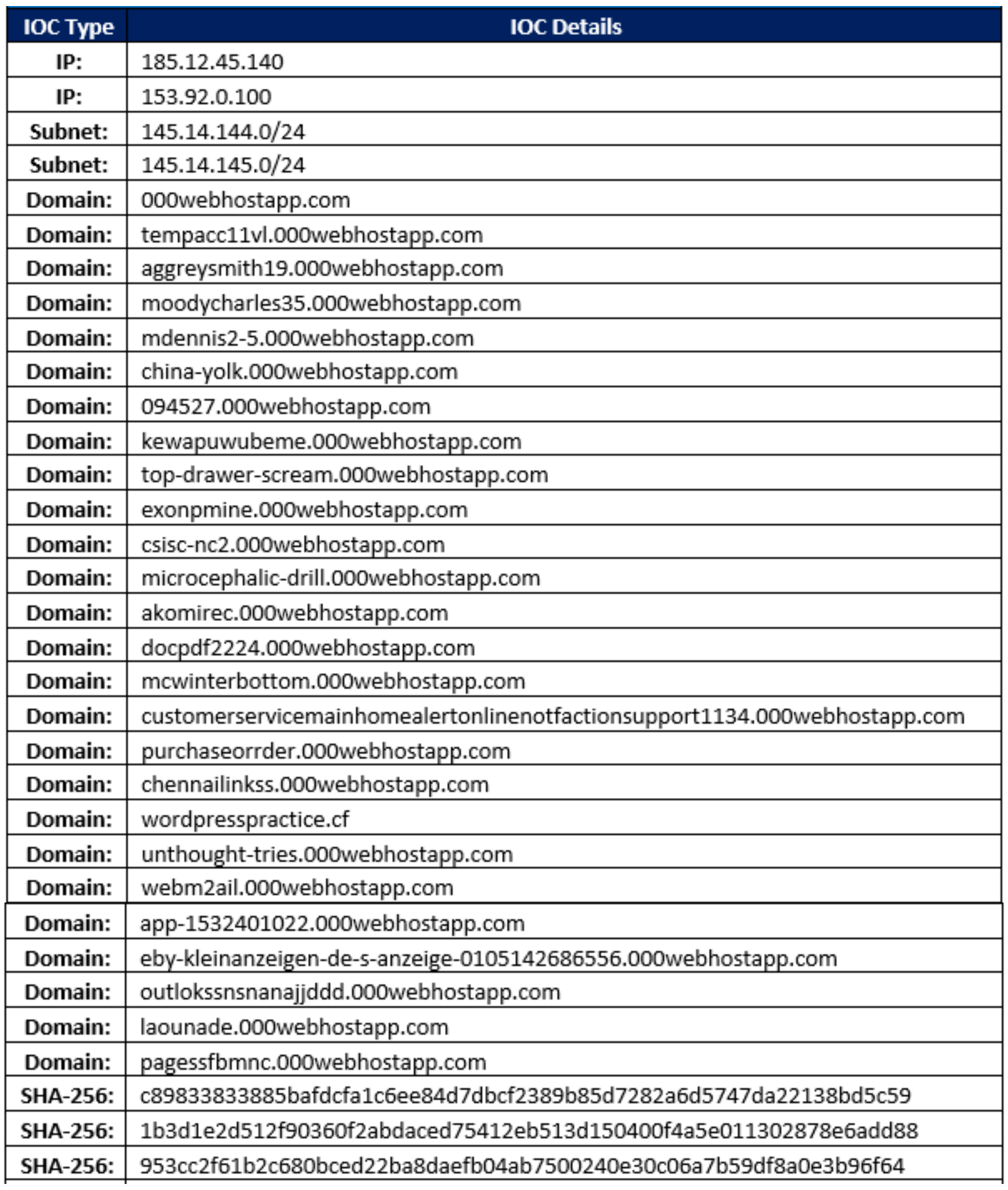
THREAT CAPABILITIES

- Shrug2 Ransomware encrypts data on the target system using randomly generated AES256 encryption key and permanently deletes shadow copy of data to prevent data recovery.
- It uses DotNetToJScript technique to load and execute Banking Trojan straight from memory without installing malicious code on hard drive.
- Banking Trojan functionality is persistent and can allow an attacker to have persistent footholds on the system.
- It can cause data loss, data breach, financial losses and disruption in business operations.

READ

- Again! A New .NET Ransomware Shrug2 Quick Heal Security Simplified
- A New .NET Ransomware Shrug2 Encrypts Files Around 76 Different Extensions GBHackers on Security

INDICATORS OF COMPROMISE



IOC Type	IOC Details
IP:	185.12.45.140
IP:	153.92.0.100
Subnet:	145.14.144.0/24
Subnet:	145.14.145.0/24
Domain:	000webhostapp.com
Domain:	tempacc11vl.000webhostapp.com
Domain:	aggreysmith19.000webhostapp.com
Domain:	moodycharles35.000webhostapp.com
Domain:	mdennis2-5.000webhostapp.com
Domain:	china-yolk.000webhostapp.com
Domain:	094527.000webhostapp.com
Domain:	kewapuwubeme.000webhostapp.com
Domain:	top-drawer-scream.000webhostapp.com
Domain:	exonpmine.000webhostapp.com
Domain:	csisc-nc2.000webhostapp.com
Domain:	microcephalic-drill.000webhostapp.com
Domain:	akomirec.000webhostapp.com
Domain:	docpdf2224.000webhostapp.com
Domain:	mcwinterbottom.000webhostapp.com
Domain:	customerservicemainhomealertonlinenotfactionsupport1134.000webhostapp.com
Domain:	purchaseorrder.000webhostapp.com
Domain:	chennailinkss.000webhostapp.com
Domain:	wordpresspractice.cf
Domain:	unthought-tries.000webhostapp.com
Domain:	webm2ail.000webhostapp.com
Domain:	app-1532401022.000webhostapp.com
Domain:	eby-kleinanzeigen-de-s-anzeige-0105142686556.000webhostapp.com
Domain:	outlokssnsnanajjddd.000webhostapp.com
Domain:	laounade.000webhostapp.com
Domain:	pagessfbmnc.000webhostapp.com
SHA-256:	c89833833885bafdcfa1c6ee84d7dbcf2389b85d7282a6d5747da22138bd5c59
SHA-256:	1b3d1e2d512f90360f2abdaced75412eb513d150400f4a5e011302878e6add88
SHA-256:	953cc2f61b2c680bced22ba8daefb04ab7500240e30c06a7b59df8a0e3b96f64