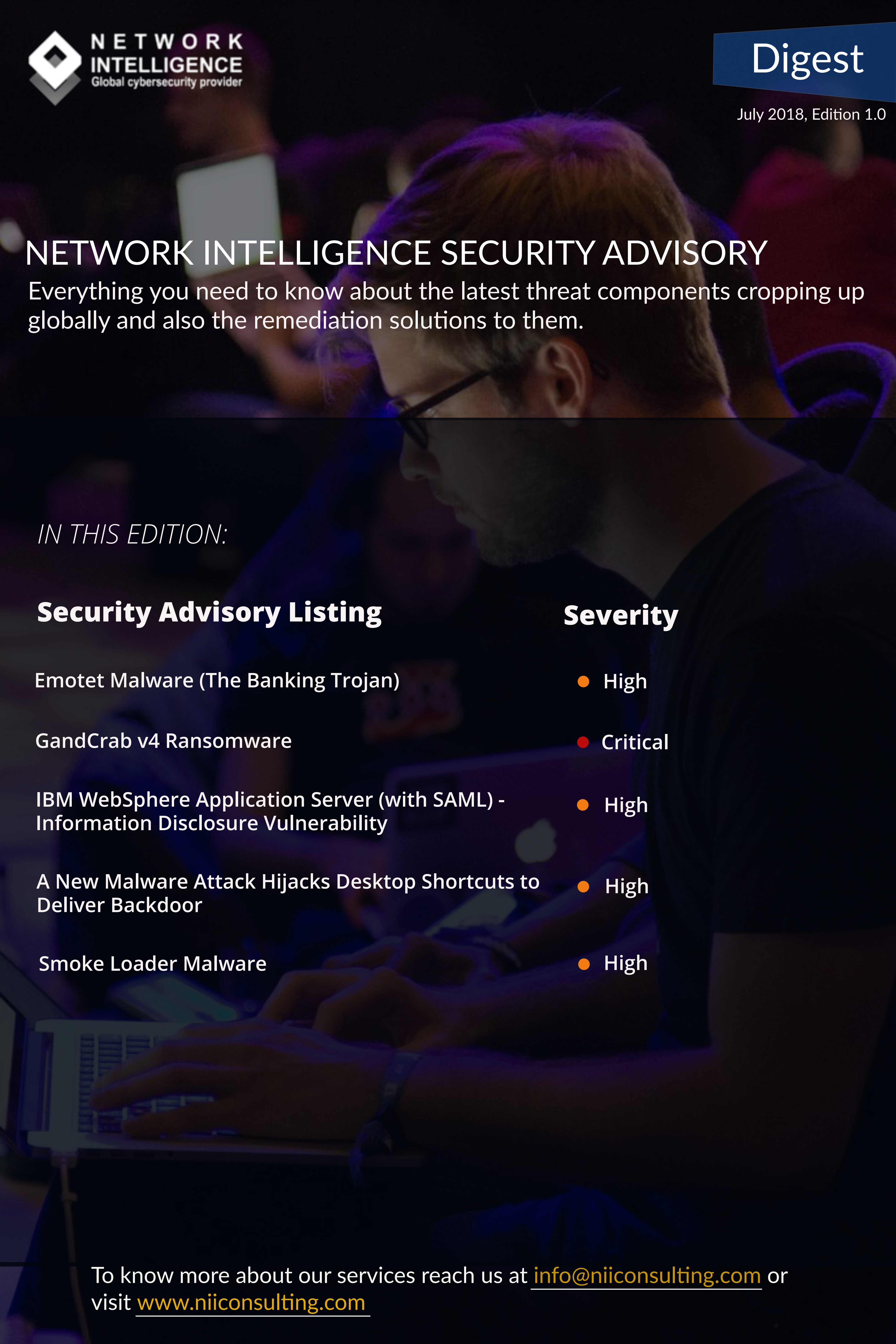


NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

July 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:

Security Advisory Listing	Severity
Emotet Malware (The Banking Trojan)	● High
GandCrab v4 Ransomware	● Critical
IBM WebSphere Application Server (with SAML) - Information Disclosure Vulnerability	● High
A New Malware Attack Hijacks Desktop Shortcuts to Deliver Backdoor	● High
Smoke Loader Malware	● High

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

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Emotet Malware (The Banking Trojan)

Severity: High

Date: June 29, 2018

IMPACT

New variant of Emotet Banking Trojan has been spotted on the radar that leverages man-in-the-browser & code inject attack techniques to steal user's banking credentials and user's data on to the C2 servers. This would result in breach of login credentials and sensitive data entered or viewed in web browsers or stored on computer.

REMEDIATION

- Ensure Microsoft Windows Workstations and Servers are up-to-date with latest security patches.
- Ensure Antivirus Signature Database is up-to-date and Antivirus scan is run on daily or weekly basis.
- Ensure all web browsers are up-to-date with latest release and meet Security Benchmark.
- Block IP/Domain/Hashes mentioned under Indicator of Compromise section below, on security devices.

INTRODUCTION

New variant of Emotet Banking Trojan has been spotted on the radar that leverages man-in-the-browser & code inject attack techniques to steal user's banking credentials and user's data on to the C2 servers. During Q1 of 2018, The malware author of Emotet had partnered with malware author of TrickBot, to modified source code of Emotet banking trojan for adding self-spreading component and was under alpha testing during April 2018. First sample of this new variant was spotted and analysed on June 11, 2018.

THREAT CAPABILITIES

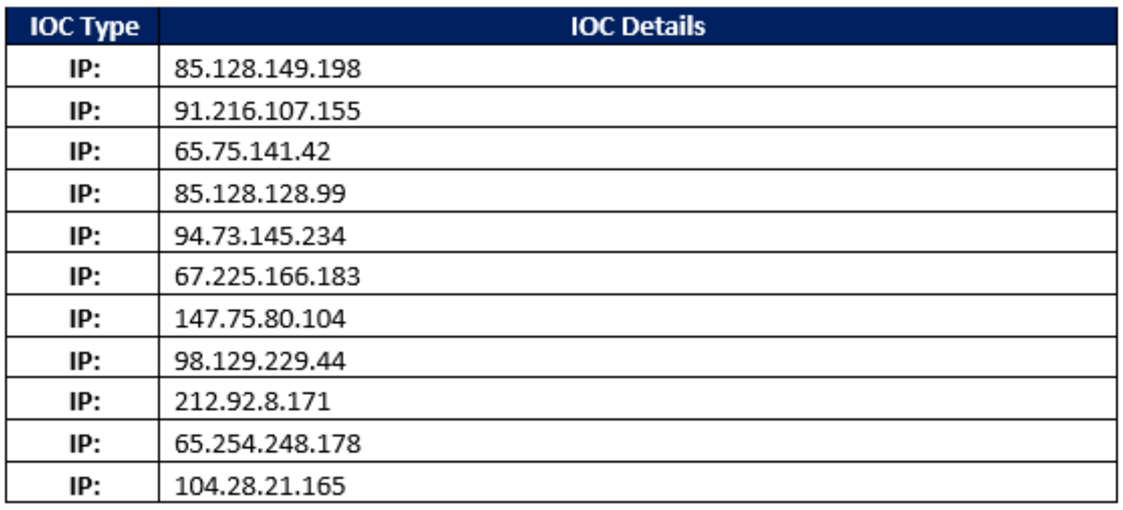
- Emotet Banking Trojan added support for a self-spreading component to improve their chances of infecting other victims on the same network.
- It drops a self-extracting RAR file on infected hosts and uses it to search & gain access to local network resources via brute-force login attempts.
- It can extract contacts from email clients and spam each victim with malicious emails.
- It allows attacker to have lateral movement inside a network, help them to collect banking credentials and steal money from bank accounts using MitB (Man-in-the-Browser) attacks.
- It is also used to collect credentials of social media accounts, and drop other malware on infected hosts.

READ

Malware analysis: decoding Emotet Malwarebytes LABS

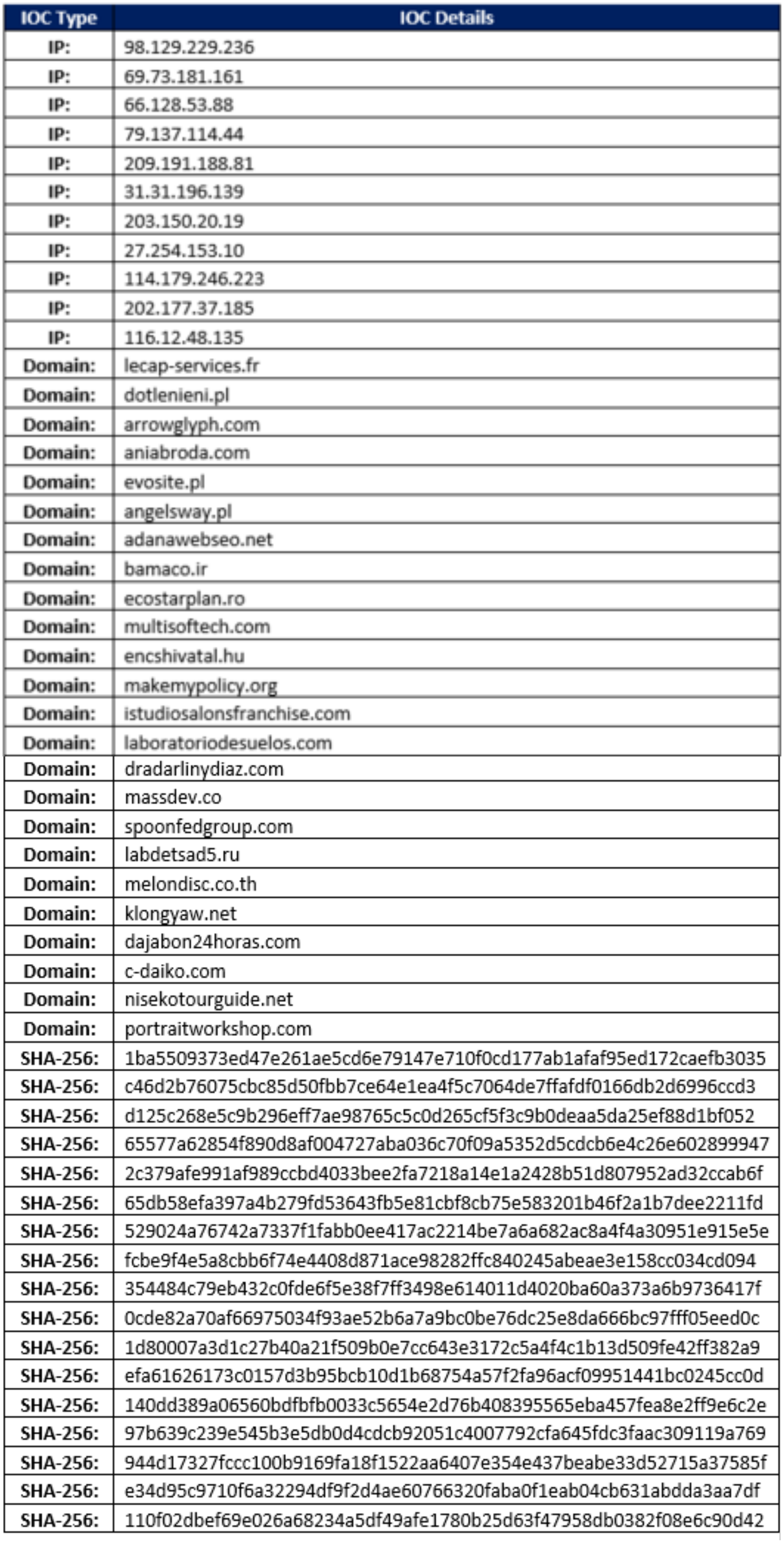
Banking Trojans Add Self-Spreading Worm Components BLEEPINGCOMPUTER

INDICATORS OF COMPROMISE



IOC Type	IOC Details
IP:	85.128.149.198
IP:	91.216.107.155
IP:	65.75.141.42
IP:	85.128.128.99
IP:	94.73.145.234
IP:	67.225.166.183
IP:	147.75.80.104
IP:	98.129.229.44
IP:	212.92.8.171
IP:	65.254.248.178
IP:	104.28.21.165

INDICATORS OF COMPROMISE



IOC Type	IOC Details
IP:	98.129.229.236
IP:	69.73.181.161
IP:	66.128.53.88
IP:	79.137.114.44
IP:	209.191.188.81
IP:	31.31.196.139
IP:	203.150.20.19
IP:	27.254.153.10
IP:	114.179.246.223
IP:	202.177.37.185
IP:	116.12.48.135
Domain:	lecap-services.fr
Domain:	dotlenieni.pl
Domain:	arrowglyph.com
Domain:	aniabroda.com
Domain:	evosite.pl
Domain:	angelsway.pl
Domain:	adanawebseo.net
Domain:	bamaco.ir
Domain:	ecostarplan.ro
Domain:	multisoftech.com
Domain:	encshivatal.hu
Domain:	makemypolicy.org
Domain:	istudiosalonsfranchise.com
Domain:	laboratoriodesuelos.com
Domain:	dradarlinydiaz.com
Domain:	massdev.co
Domain:	spoonfedgroup.com
Domain:	labdetsad5.ru
Domain:	melondisc.co.th
Domain:	klongyaw.net
Domain:	dajabon24horas.com
Domain:	c-daiko.com
Domain:	nisekotourguide.net
Domain:	portraitworkshop.com
SHA-256:	1ba5509373ed47e261ae5cd6e79147e710f0cd177ab1afaf95ed172caefb3035
SHA-256:	c46d2b76075cbc85d50fbb7ce64e1ea4f5c7064de7ffafdf0166db2d6996ccd3
SHA-256:	d125c268e5c9b296eff7ae98765c5c0d265cf5f3c9b0deaa5da25ef88d1bf052
SHA-256:	65577a62854f890d8af004727aba036c70f09a5352d5cdcb6e4c26e602899947
SHA-256:	2c379afe991af989ccbd4033bee2fa7218a14e1a2428b51d807952ad32ccab6f
SHA-256:	65db58efa397a4b279fd53643fb5e81cbf8cb75e583201b46f2a1b7dee2211fd
SHA-256:	529024a76742a7337f1fabb0ee417ac2214be7a6a682ac8a4f4a30951e915e5e
SHA-256:	fcbe9f4e5a8cbb6f74e4408d871ace98282ffc840245abeae3e158cc034cd094
SHA-256:	354484c79eb432c0fde6f5e38f7ff3498e614011d4020ba60a373a6b9736417f
SHA-256:	0cde82a70af66975034f93ae52b6a7a9bc0be76dc25e8da666bc97fff05eed0c
SHA-256:	1d80007a3d1c27b40a21f509b0e7cc643e3172c5a4f4c1b13d509fe42ff382a9
SHA-256:	efa61626173c0157d3b95bcb10d1b68754a57f2fa96acf09951441bc0245cc0d
SHA-256:	140dd389a06560bdfbfb0033c5654e2d76b408395565eba457fea8e2ff9e6c2e
SHA-256:	97b639c239e545b3e5db0d4cdcb92051c4007792cfa645fdc3faac309119a769
SHA-256:	944d17327fccc100b9169fa18f1522aa6407e354e437beabe33d52715a37585f
SHA-256:	e34d95c9710f6a32294df9f2d4ae60766320faba0f1eab04cb631abdda3aa7df
SHA-256:	110f02dbef69e026a68234a5df49afe1780b25d63f47958db0382f08e6c90d42

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

GandCrab v4 Ransomware

Severity: Critical

Date: July 4, 2018

IMPACT

This ransomware attack poses a serious risk of data loss, which will directly impact production line, disrupt business operations and cause financial loss.

REMEDIATION

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

INTRODUCTION

A new variant of GandCrab Ransomware (aka, GandCrab v4) has been released and it is being distributed via fake crack sites. The GandCrab v4 Ransomware demanding $1200 USD (in DASH cryptocurrency) as a ransom amount from victims and there is no way to decrypt data that are encrypted by GandCrab v4 Ransomware.

THREAT CAPABILITIES

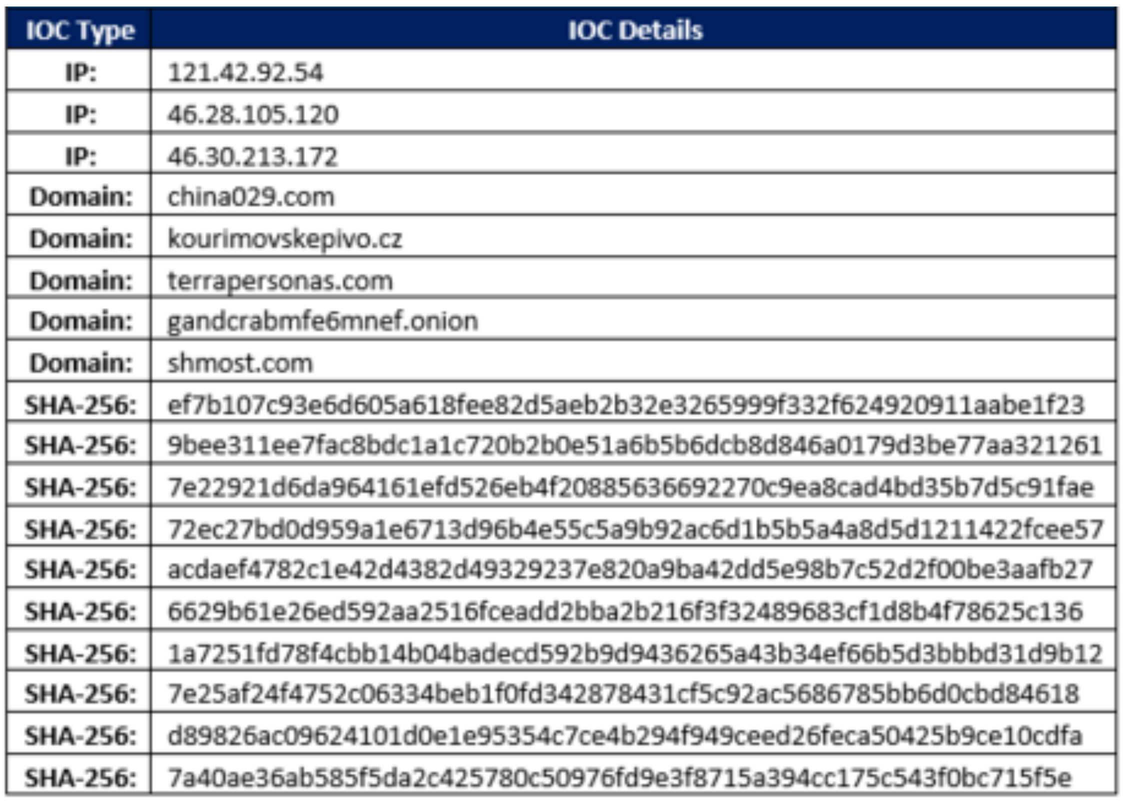
- GandCrab v4 Ransomware will scan the computer and any network shares for files to encrypt.
- When scanning for network shares, it will enumerate all shares on the network and not just mapped drives.
- When it encounters a targeted file, it will encrypt the file and then append the .KRAB extension to the encrypted file name.

READ

GandCrab V4 Released With the New .KRAB Extension for Encrypted Files

BLEEPINGCOMPUTER

INDICATORS OF COMPROMISE



IOC Type	IOC Details
IP:	121.42.92.54
IP:	46.28.105.120
IP:	46.30.213.172
Domain:	china029.com
Domain:	kourimovskepivo.cz
Domain:	terrapersonas.com
Domain:	gandcrabmfe6mnef.onion
Domain:	shmost.com
SHA-256:	ef7b107c93e6d605a618fee82d5aeb2b32e3265999f332f624920911aabe1f23
SHA-256:	9bee311ee7fac8bdc1a1c720b2b0e51a6b5b6dcb8d846a0179d3be77aa321261
SHA-256:	7e22921d6da964161efd526eb4f20885636692270c9ea8cad4bd35b7d5c91fae
SHA-256:	72ec27bd0d959a1e6713d96b4e55c5a9b92ac6d1b5b5a4a8d5d1211422fcee57
SHA-256:	acdaef4782c1e42d4382d49329237e820a9ba42dd5e98b7c52d2f00be3aafb27
SHA-256:	6629b61e26ed592aa2516fceadd2bba2b216f3f32489683cf1d8b4f78625c136
SHA-256:	1a7251fd78f4cbb14b04badecd592b9d9436265a43b34ef66b5d3bbbd31d9b12
SHA-256:	7e25af24f4752c06334beb1f0fd342878431cf5c92ac5686785bb6d0cbd84618
SHA-256:	d89826ac09624101d0e1e95354c7ce4b294f949ceed26feca50425b9ce10cdfa
SHA-256:	7a40ae36ab585f5da2c425780c50976fd9e3f8715a394cc175c543f0bc715f5e

IBM WebSphere Application Server (with SAML) - Information Disclosure Vulnerability

Severity: High

Date: July 5, 2018

IMPACT

IBM WebSphere Application Server using malformed SAML responses from the SAML identity provider could allow a remote attacker to obtain sensitive information.

REMEDIATION

Please download the Prerequisite UpdateInstaller before applying following available Patches to respective WebSphere Application Server:

1.For WebSphere Application Server (Traditional / Hypervisor) Edition v9.0.0.0 through v9.0.0.8, apply available Patches 9.0.0.0-WS-WASProd-IFPI78804 or upgrade to v9.0.0.9 or later.

2.For WebSphere Application Server (Traditional / Hypervisor) Edition V8.5.0.0 through 8.5.5.13, apply available Patches 8.5.5.0-WS-WASProd-IFPI78804 or upgrade to 8.5.5.14 or later.

3.For WebSphere Application Server (Traditional / Hypervisor) Edition V8.0.0.0 through 8.0.0.15, apply available Patches 8.0.0.4-WS-WASProd-IFPI78804 or upgrade to v9.0.0.9 or later.

Important: IBM WebSphere Application Server v7.0 and v8.0 are no longer in full support. **IBM's Statement** recommends upgrading to a fixed or supported version of the product.

VULNERABILITY

This vulnerability affects the following versions and releases of IBM WebSphere Application Server:

- Version 9.0
- Version 8.5
- Version 8.0
- Version 7.0

READ

- Security Bulletin: Information disclosure in WebSphere Application Server with SAML (CVE-2018-1614) IBM
- PI78804: Information disclosure in WebSphere Application Server with SAML (CVE-2018-1614) IBM
- IBM WebSphere Application Server Unspecified Flaw in SAML Response Processing Lets Remote Users Obtain Potentially Sensitive Information on the Target System Security tracker

A New Malware Attack Hijacks Desktop Shortcuts to Deliver Backdoor

Severity: High

Date: July 5, 2018

IMPACT

A new malware attack that uses Word documents embedded with malicious macros to trick users into executing a backdoor program, and then steal information from infected computers and sent it to email accounts via the SMTP servers. This would result in breach of login credentials and sensitive data stored in web browser or stored on computer.

REMEDIATION

- Ensure Microsoft Windows Workstations and Servers are up-to-date with latest security patches.
- Ensure Antivirus Signature Database is up-to-date and Antivirus scan is run on daily or weekly basis.
- Ensure Macro is disabled in Microsoft Office Product.
- Block URL/Hashes mentioned under Indicator of Compromise section below, on security devices.

INTRODUCTION

A new malware attack that uses Word documents embedded with malicious macros which modifies legitimate application shortcut files from the Windows desktop to trick users into executing a backdoor program, and then steal information from infected computers and sent it to email accounts via the SMTP servers of rambler.ru and meta.ua.

THREAT CAPABILITIES

- This new malware attack downloads a backdoor program from Google Drive or GitHub, then scans the computer's desktop for shortcuts of popular applications: Skype, Google Chrome, Mozilla Firefox, Opera and Internet Explorer. If these shortcuts are found, the script replaces their target links with the path to the newly downloaded backdoor program.
- The downloaded backdoor program also tries to masquerade as one of those legitimate applications to evade detection.
- It also creates a rogue Windows service called "WPM Provider Host" that will run in the background and download additional components such as WinRAR and the Ammyy Admin remote administration tool, to steal information from infected computers.

READ

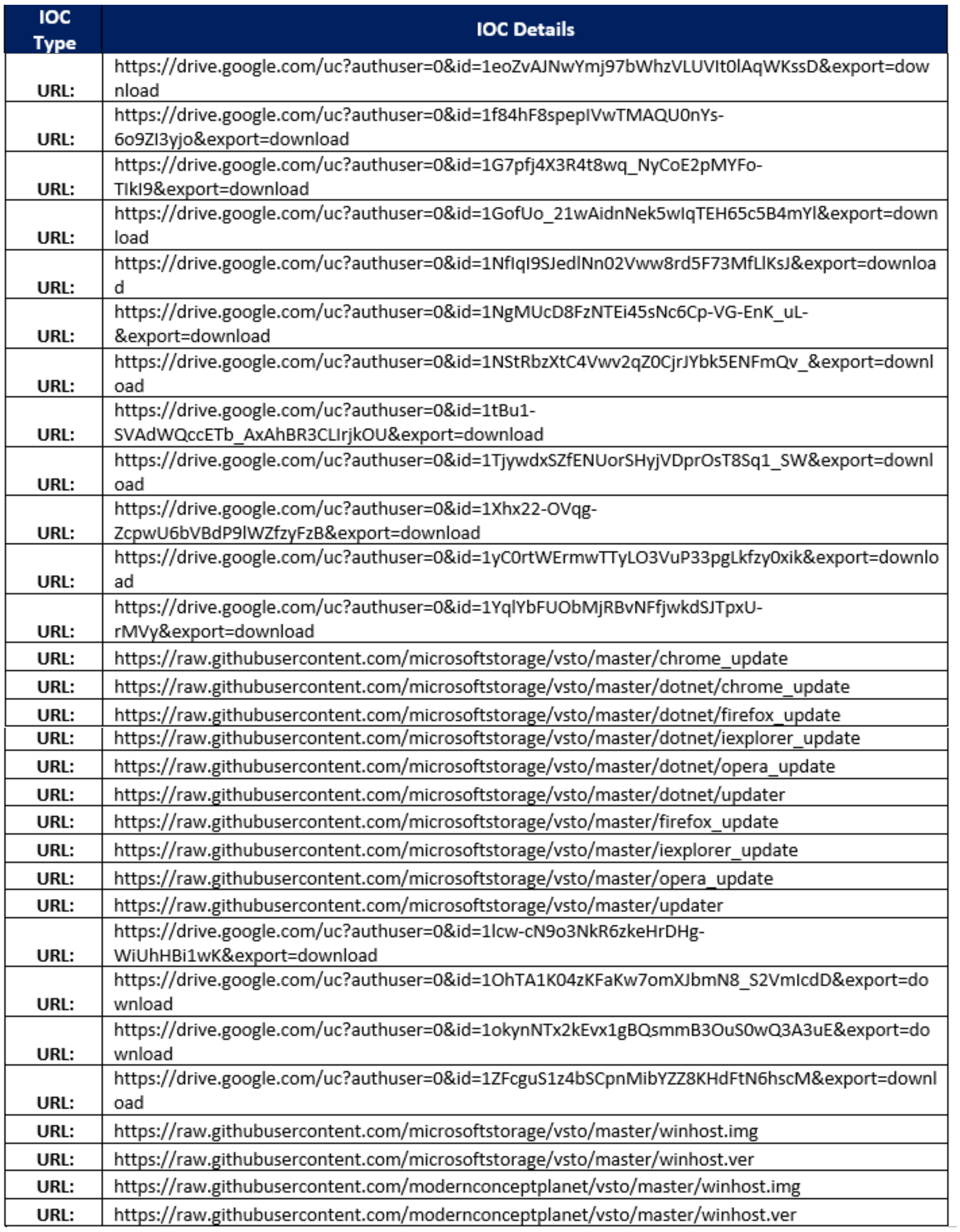
Malicious Macro Hijacks Desktop Shortcuts to Deliver Backdoor. TREND MICRO

Macros-based Attack Deploys Malware by Hijacking Desktop Shortcuts. SECURITY BOULEVARD

INDICATORS OF COMPROMISE

IOC Type	IOC Details
SHA-256:	0181a985897f1fa66ede98cc04e97b05387743de198c2dcf4667fa4fde7779c1
SHA-256:	20b05a17623a7e74f7cfe4296ba79cff8ca6b3ea64f404661b7bc46ab603511c
SHA-256:	2864b1b7417aacc13a4277d8cb9c94b5a04420f6ccc1cc4dfd3be4d369406383
SHA-256:	2b3cd4d85b2b1f22d88db07352fb9e93405f395e7d0cfe96490ea2bc03a8c5ff
SHA-256:	3b85e737965020d82cdc0890f1243732b71977117cdf310554e9dd91b78bfe63
SHA-256:	451c4c3fbf5aec103833fa98d942b1876d9ce84575a00757562489921bc1d396
SHA-256:	45b2580db6d13720014753813eb69c1aa0effbd100bb80e5a07d75447489ba0f
SHA-256:	7730a98fd698f1043184992f1ca349ea1bdfd33d43a0ece2cd88f9f6da2e37d1
SHA-256:	804d883661ba51cec97135f9f33c1fa9084384783d59a4f55d496e2901c20289
SHA-256:	96a4f844d7102d0ee757caa1719f1cd95d1386e61eb7c694020d6cf14b546880
SHA-256:	9eac92bec146ce9cef096105f6531f2ee4c2e1a14507f069728a1022ecdcdedd
SHA-256:	a4b25e5e72fc552e30391d7cd8182af023dc1084641d93b7fa6f348e89b29492
SHA-256:	a9fc2b6f8bc339742268bac6c02843011ebb670114a786a71ff0fa65397ac9c6
SHA-256:	c57bf08c414900b5b4ad907272a606d6695c14dc2acc0264eca53840eee3f3f4
SHA-256:	c9b7c2189d3cea05a666c45043812d832bed60cfcb8a97222bca9afc53b3d229
SHA-256:	cc60dae1199c72543dd761c921397f6e457ff0440da5b4451503bfca9fb0c730
SHA-256:	d904495737dfe33599c0c408855f6d0dd9539be4b989eb5ab910eb6ab076d9ef

INDICATORS OF COMPROMISE



IOC Type	IOC Details
URL:	https://drive.google.com/uc?authuser=0&id=1eoZvAJNwYmj97bWhzVLUVIt0lAqWKssD&export=download
URL:	https://drive.google.com/uc?authuser=0&id=1f84hF8spepIVwTMAQU0nYs-6o9ZI3yjo&export=download
URL:	https://drive.google.com/uc?authuser=0&id=1G7pfj4X3R4t8wq_NyCoE2pMYFo-TIkI9&export=download
URL:	https://drive.google.com/uc?authuser=0&id=1GofUo_21wAidnNek5wIqTEH65c5B4mYl&export=download
URL:	https://drive.google.com/uc?authuser=0&id=1NfIqI9SJedlNn02Vww8rd5F73MfLlKsJ&export=download
URL:	https://drive.google.com/uc?authuser=0&id=1NgMUcD8FzNTEi45sNc6Cp-VG-EnK_uL-&export=download
URL:	https://drive.google.com/uc?authuser=0&id=1NStRbzXtC4Vwv2qZ0CjrJYbk5ENFmQv_&export=download
URL:	https://drive.google.com/uc?authuser=0&id=1tBu1-SVAdWQccETb_AxAhBR3CLIrjkOU&export=download
URL:	https://drive.google.com/uc?authuser=0&id=1TjywdxSZfENUorSHyjVDprOsT8Sq1_SW&export=download
URL:	https://drive.google.com/uc?authuser=0&id=1Xhx22-OVqg-ZcpwU6bVBdP9lWZfzyFzB&export=download
URL:	https://drive.google.com/uc?authuser=0&id=1yC0rtWErmwTTyLO3VuP33pgLkfzy0xik&export=download
URL:	https://drive.google.com/uc?authuser=0&id=1YqlYbFUObMjRBvNFfjwkdSJTpxU-rMVy&export=download
URL:	https://raw.githubusercontent.com/microsoftstorage/vsto/master/chrome_update
URL:	https://raw.githubusercontent.com/microsoftstorage/vsto/master/dotnet/chrome_update
URL:	https://raw.githubusercontent.com/microsoftstorage/vsto/master/dotnet/firefox_update
URL:	https://raw.githubusercontent.com/microsoftstorage/vsto/master/dotnet/iexplorer_update
URL:	https://raw.githubusercontent.com/microsoftstorage/vsto/master/dotnet/opera_update
URL:	https://raw.githubusercontent.com/microsoftstorage/vsto/master/dotnet/updater
URL:	https://raw.githubusercontent.com/microsoftstorage/vsto/master/firefox_update
URL:	https://raw.githubusercontent.com/microsoftstorage/vsto/master/iexplorer_update
URL:	https://raw.githubusercontent.com/microsoftstorage/vsto/master/opera_update
URL:	https://raw.githubusercontent.com/microsoftstorage/vsto/master/updater
URL:	https://drive.google.com/uc?authuser=0&id=1lcw-cN9o3NkR6zkeHrDHg-WiUhHBi1wK&export=download
URL:	https://drive.google.com/uc?authuser=0&id=1OhTA1K04zKFaKw7omXJbmN8_S2VmIcdD&export=download
URL:	https://drive.google.com/uc?authuser=0&id=1okynNTx2kEvx1gBQsmmB3OuS0wQ3A3uE&export=download
URL:	https://drive.google.com/uc?authuser=0&id=1ZFcguS1z4bSCpnMibYZZ8KHdFtN6hscM&export=download
URL:	https://raw.githubusercontent.com/microsoftstorage/vsto/master/winhost.img
URL:	https://raw.githubusercontent.com/microsoftstorage/vsto/master/winhost.ver
URL:	https://raw.githubusercontent.com/modernconceptplanet/vsto/master/winhost.img
URL:	https://raw.githubusercontent.com/modernconceptplanet/vsto/master/winhost.ver

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Smoke Loader Malware

Severity: High

Date: July 5, 2018

IMPACT

A new strain of malware called Smoke Loader uses TrickBot's (Banking Trojan) C2 Servers for carrying out malware operations. It leverages the PROPagate injection technique to inject code which downloads and executes additional malwares on the compromised system and evade detection. This would result in breach of login credentials and sensitive data stored on computer.

REMEDIATION

- Ensure Microsoft Windows Workstations and Servers are up-to-date with 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.

INTRODUCTION

A new strain of malware called Smoke Loader have been active since June 05, 2018 and uses TrickBot's (Banking Trojan) C2 Servers for carrying out malware operations. This malware drops additional malwares such as Banking Trojan, Keylogger and ransomware as part of infection chain and C2 operations. Malware authors of Smoke Loader and TrickBot had collaborated to develop this malware that leverages the PROPagate injection technique to inject code which downloads and executes additional malwares on the compromised computer and evade detection.

THREAT CAPABILITIES

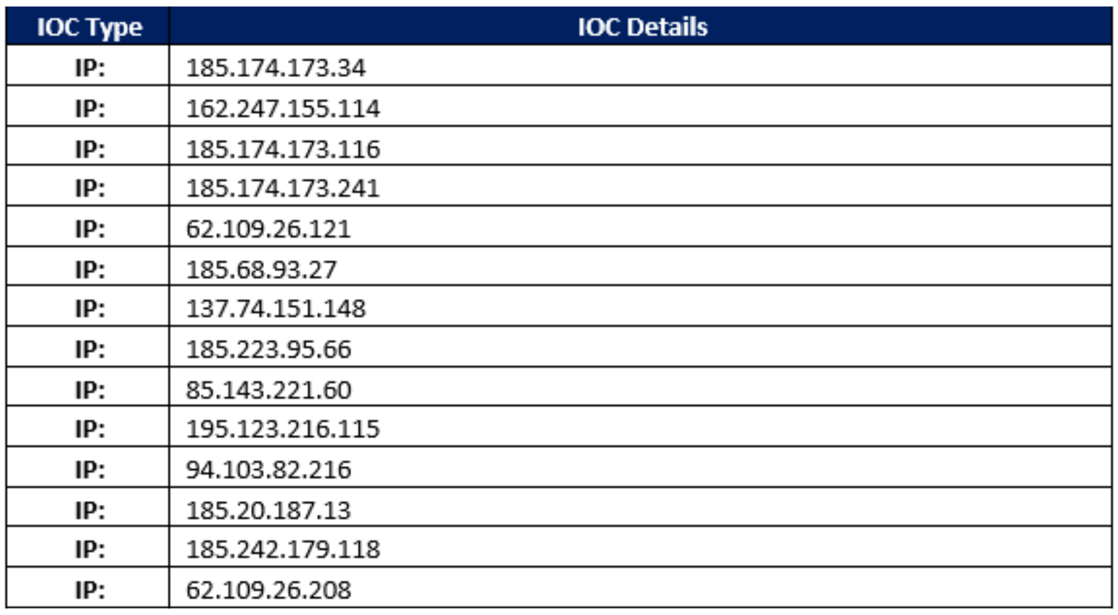
- Smoke Loader is primarily used as a downloader to drop and execute additional malware like ransomware, Banking Trojan, Keylogger and cryptocurrency miners, as part of infection chain and C2 operations.
- It leverages the PROPagate injection technique to inject code which downloads and executes additional malwares on the compromised system and evade detection.
- It uses TrickBot's (Banking Trojan) C2 Servers for carrying out malware operations.

READ

Smoking Guns - Smoke Loader learned new tricks TALOS

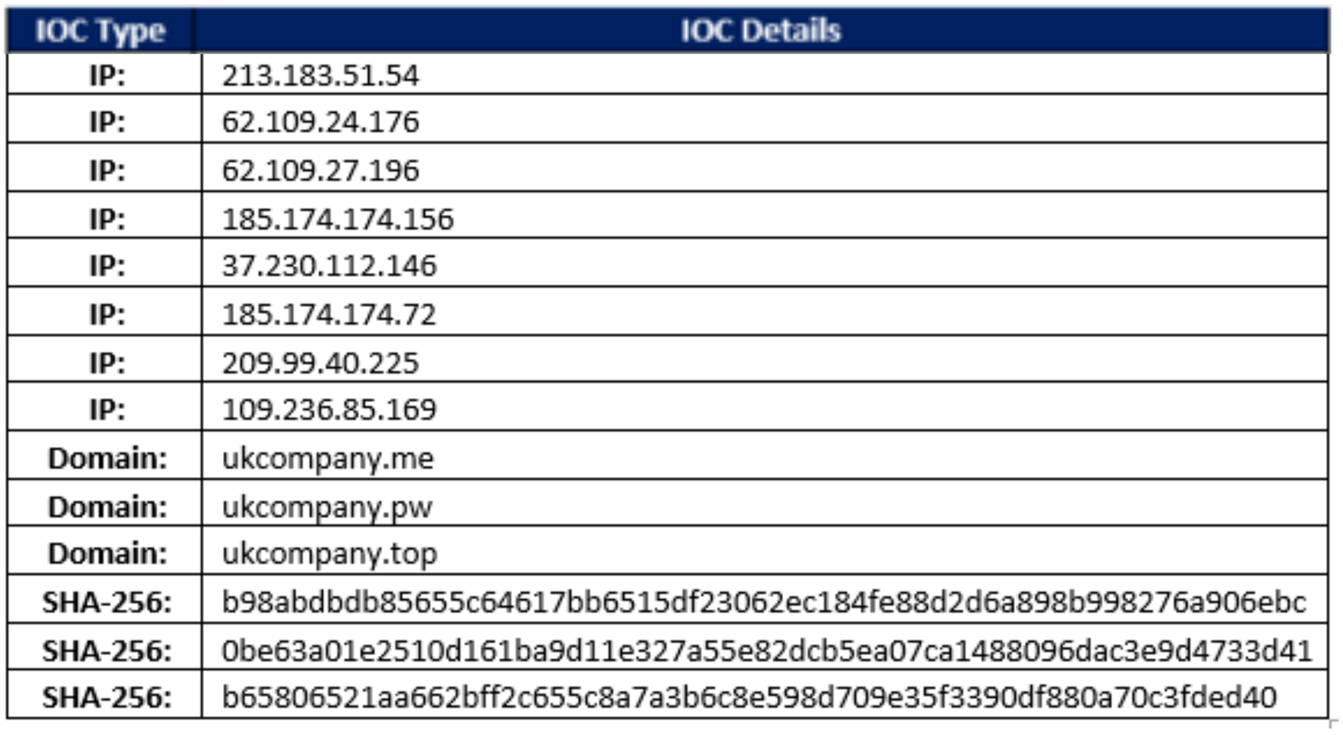
This password-stealing malware just added a new way to infect your PC Windows TenForums

INDICATORS OF COMPROMISE



IOC Type	IOC Details
IP:	185.174.173.34
IP:	162.247.155.114
IP:	185.174.173.116
IP:	185.174.173.241
IP:	62.109.26.121
IP:	185.68.93.27
IP:	137.74.151.148
IP:	185.223.95.66
IP:	85.143.221.60
IP:	195.123.216.115
IP:	94.103.82.216
IP:	185.20.187.13
IP:	185.242.179.118
IP:	62.109.26.208

INDICATORS OF COMPROMISE



IOC Type	IOC Details
IP:	213.183.51.54
IP:	62.109.24.176
IP:	62.109.27.196
IP:	185.174.174.156
IP:	37.230.112.146
IP:	185.174.174.72
IP:	209.99.40.225
IP:	109.236.85.169
Domain:	ukcompany.me
Domain:	ukcompany.pw
Domain:	ukcompany.top
SHA-256:	b98abdbdb85655c64617bb6515df23062ec184fe88d2d6a898b998276a906ebc
SHA-256:	0be63a01e2510d161ba9d11e327a55e82dcb5ea07ca1488096dac3e9d4733d41
SHA-256:	b65806521aa662bff2c655c8a7a3b6c8e598d709e35f3390df880a70c3fded40