NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

September 2018, Edition 2.0

NETWORK INTELLIGENCE SECURITY ADVISORY

The major security news items of the month - major threats and breaches. The advisory also includes IOCs and remediation steps.

IN THIS EDITION:

Security Advisory Listing	Severity
Xbash Malware with Ransomware and Cryptomining capabilities, found targeting vulnerable Linux and Microsoft Windows Servers	Critical
Adobe released security update for a critical vulnerability in Adobe Acrobat and Adobe Reader	Critical
Mass exploitation campaign found targeting WordPress vulnerability CVE-2018-12895, to compromise WordPress websites through malicious code injection	High
An Exploitation Campaign found targeting Microsoft Scripting Engine Memory Corruption Vulnerability (CVE-2018-8373)	High
APT Threat Actors are actively Exploiting IT Infrastructure of Managed Service Providers and their customers	Critical

ALSO INSIDE

Data Breach Highlights

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

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Xbash Malware with Ransomware and Cryptomining capabilities, found targeting vulnerable Linux and Microsoft Windows Servers

Severity: Critical

Date: September 18, 2018

IMPACT

This poses a serious risk of data loss and disruption in business operations.

REMEDIATION

- Ensure Microsoft Windows Servers and Linux Servers are up-to-date with the latest security patches.
- Ensure Antivirus Signature Database is up-to-date and Antivirus scan is run on a daily or weekly basis.
- Ensure proper access controls are in place to restrict inbound connection from Public IP to destination ports running critical services.
- Block IP/Email/Domain/Hashes mentioned under Threat Indicators section below, on security devices.

INTRODUCTION

This Xbash Malware which includes ransomware and cryptomining capabilities, found targeting vulnerable Linux as well as Microsoft Windows Servers on global scale. It takes advantage of weak passwords and unpatched vulnerabilities, to spread across the corporate network more quickly as compare to typical worm infection. It deletes database file managed by Relational Database Management Systems such as Microsoft SQL Server, MySQL community Server, Oracle Database, IBM DB2, MongoDB, PostgreSQL, SQLite, Redis, Elasticsearch, MariaDB, Memcached, etc. It also causes high system resource utilization while mining cryptocurrency on compromised servers.

THREAT CAPABILITIES

- This Xbash Malware which includes ransomware and cryptomining capabilities, targets vulnerable Linux and Microsoft Windows Servers.
- It takes advantage of weak passwords and unpatched vulnerabilities, to spread across the corporate network.
- It deletes database files managed by Relational Database Management Systems such as Microsoft SQL Server, MySQL community Server, Oracle Database, IBM DB2, MongoDB, PostgreSQL, SQLite, Redis, Elasticsearch, MariaDB, Memcached, etc. It also causes high system resource utilization while mining cryptocurrency on compromised servers.
- It probes for following services and performs Brute Force attack
  - HTTP: 80, 8080, 8888, 8000, 8001, 8088
  - VNC: 5900, 5901, 5902, 5903
  - MySQL: 3306
  - Memcached: 11211
  - MySQL/MariaDB: 3309, 3308,3360 3306, 3307, 9806, 1433
  - FTP: 21
  - Telnet: 23, 2323
  - PostgreSQL: 5432
  - Redis: 6379, 2379
  - ElasticSearch: 9200
  - MongoDB: 27017
  - RDP: 3389
  - UPnP/SSDP: 1900
  - NTP: 123
  - DNS: 53
  - SNMP: 161
  - LDAP: 389
  - Rexec: 512
  - Rlogin: 513
  - Rsh: 514
  - Rsync: 873
  - Oracle database: 1521

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Xbash Malware with Ransomware and Cryptomining capabilities, found targeting vulnerable Linux and Microsoft Windows Servers

Severity: Critical

Date: September 18, 2018

READ

•Iron Group suspected in creation of Xbash all-in-one malware

• Xbash Combines Botnet, Ransomware, Coinmining in Worm that Targets Linux and Windows

IP ADDRESSES

- 142.44.215.177
- 144.217.61.147
- 104.24.106.22
- 104.24.107.22
- 104.24.98.120
- 104.24.99.120
- 104.27.137.249
- 104.27.136.249
- 104.27.143.6
- 104.27.142.6
- 104.27.138.117
- 104.27.139.117
- 104.24.126.240
- 104.24.127.240
- 104.24.107.247
- 104.24.106.247
- 104.24.109.199
- 104.24.108.199
- 45.76.228.115
- 104.24.126.99
- 104.24.127.99
- 185.199.108.153
- 104.27.166.65
- 104.27.167.65

DOMAINS

- ejectrift.censys.xyz
- scan.censys.xyz
- api.leakingprivacy.tk
- news.realnewstime.xyz
- scan.realnewstime.xyz
- news.realtimenews.tk
- scanaan.tk
- scan.3g2upl4pq6kufc4m.tk
- scan.vfk2k5s5tfjr27tz.tk
- scan.blockbitcoin.tk
- blockbitcoin.com
- 3g2upl4pq6kufc4m.tk
- e3sas6tzvehwgpak.tk
- xmr.enjoytopic.tk
- png.realtimenews.tk
- daknobcq4zal6vbm.tk
- d3goboxon32grk2l.tk

EMAILS

- backupsql@protonmail.com
- backupsql@pm.me
- backupdatabase@pm.me

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Adobe released security update for a critical vulnerability in Adobe Acrobat and Adobe Reader

Severity: Critical

Date: September 20, 2018

IMPACT

On successful exploitation of this vulnerability, it would allow remote attacker to execute malicious code in context of user account.

- CVE-2018-12848
- CVE-2018-12849
- CVE-2018-12850
- CVE-2018-12801
- CVE-2018-12840
- CVE-2018-12778
- CVE-2018-12775

REMEDIATION

- Kindly upgrade Acrobat Reader and Adobe Reader to latest version.

INTRODUCTION

Adobe released security update for a critical Arbitrary Code Execution vulnerability (CVE-2018-12848) in Adobe Acrobat and Adobe Reader. The successful exploitation of this vulnerability would allow the remote attacker to execute malicious code in context of user account.
As per current Threat Landscape, exploitation of this vulnerability is more likely to be adopted by malware attack during upcoming weeks.

VULNERABILITY

This vulnerability affected following Adobe Products

- Acrobat DC (Continuous) 2018.011.20058 and earlier versions
- Acrobat Reader DC (Continuous) 2018.011.20058 and earlier versions
- Acrobat 2017 (Classic 2017) 2017.011.30099 and earlier versions
- Acrobat Reader 2017 (Classic 2017) 2017.011.30099 and earlier versions
- Acrobat DC (Classic 2015) 2015.006.30448 and earlier versions
- Acrobat Reader DC (Classic 2015) 2015.006.30448 and earlier versions

READ

- Critical Security Update Released for Adobe Reader and Acrobat — BLEEPINGCOMPUTER
- Security bulletin for Adobe Acrobat and Reader | APSB18-34 — Adobe

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Mass exploitation campaign found targeting WordPress vulnerability CVE-2018-12895, to compromise WordPress websites through malicious code injection

Severity: High

Date: September 21, 2018

REMEDIATION

- Kindly upgrade WordPress Platforms to latest version.
- Ensure proper access controls are in place to restrict unauthorized access to directories of WordPress websites.
- Ensure strong and complex password is assigned to WordPress web admin and linked website management platform.
- Configuration Review and Code Review are strongly recommended for WordPress website and web hosting server.
- During Code Review, kindly check for any malicious code pattern similar to Code Pattern mentioned in IOCs
- Kindly Block mentioned IP/IP Subnet/Domain/Hashes, on security devices.

IP ADDRESSES

- 137.74.150.112
- 51.255.157.138
- 37.139.5.74
- 23.163.0.39
- 88.99.64.55
- 190.97.167.109
- 162.251.82.249
- 162.251.82.124
- 162.251.82.246
- 162.251.82.247
- 162.251.82.118
- 162.251.82.119
- 162.251.82.251
- 162.251.82.123
- 162.251.82.250
- 162.251.82.122

IP SUBNETS

- 162.251.80.0/22
- 162.251.84.0/23
- 162.251.86.0/24

DOMAINS

- examhome.net
- uustoughtonma.org
- mp3menu.org
- ejyoklygase.tk
- voipnewswire.net
- allyouwant.online
- 1a7ea920.bitcoin-dns.hosting
- a8332f3a.bitcoin-dns.hosting
- ad636824.bitcoin-dns.hosting
- c358ea2d.bitcoin-dns.hosting

HASHES (SHA-256)

93a3fbc7d0bd1b67d744dd27889a2d2a4761cf4638284e7094b55282048b814d
0173df8e5f7a7380d1a2926cc2027238e37f8542aea0c41ccbee5064a3fd8a4f
d33e4cc358ea8706c2e16f724b7d935f5c41a3612d4383d4b8ce198aaabdf3da

CODE PATTERN

Injected blurb (partial):
String.fromCharCode(118, 97, 114, 32, 115, 111, 109
eval(String.fromCharCode(118, 97, 114, 32

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

An Exploitation Campaign found targeting Microsoft Scripting Engine Memory Corruption Vulnerability (CVE-2018-8373)

Severity: High

Date: September 26, 2018

REMEDIATION

- Ensure Microsoft Windows Workstations and Servers are up-to-date with latest the Security Patches.
- Ensure Antivirus program and Virus Signature Database are up-to-date.
- Ensure patches for Microsoft VBScript Engine Vulnerabilities (CVE-2018-8373, CVE-2018-8242, CVE-2018-8174) are applied on Windows Platforms.
- Ensure VBScript execution in Internet Explorer is Disable.
- Ensure Macros are Disabled in Microsoft Office Product.
- Ensure proper access controls are in place to restrict inbound connections from Public IP to TCP/IP Protocol running critical services.
- Ensure internet facing devices, applications and services are using strong & complex passwords.
- Kindly Block mentioned IP/Domain/Hashes, on security devices.

IP ADDRESSES

- 54.191.17.130
- 52.33.221.185

DOMAINS

- myswcd.com
- gdmdata.com

APT Threat Actors are actively Exploiting IT Infrastructure of Managed Service Providers and their customers

Severity: Critical

Date: October 04, 2018

RECOMMENDATIONS FOR OPERATIONAL CONTROL

- Create a baseline for system and network behaviour to make it easier to track anomalies within the collected logs.
- Review network device configurations every six months. And also, review the active configurations of network devices for unauthorized settings.
- Review network environment Group Policy Objects (GPOs) every six months. And also, review GPOs for unauthorized settings.
- Continuously monitor and investigate SIEM appliance alerts. All events should be investigated and documented for future reference.
- Periodically review SIEM appliance alert thresholds every three months. Thresholds should be updated to reflect changes, such as new systems, activity variations, and new or old services being used within the network environment.
- Review privileged account groups weekly to identify any unauthorized modifications.
- Disable or remove inactive accounts that have not been active within a certain period.
- Regularly update software and operating systems which can mitigate known vulnerabilities and offering new protections.

RECOMMENDATIONS FOR ACCOUNT CONFIGURATION

- Ensure MSP accounts are not assigned to the Enterprise Administrator (EA) or Domain Administrator (DA) groups.
- Restrict MSP accounts to only the systems they manage. Administrator access to these systems should be avoided when possible.
- Ensure MSP account passwords adhere to organizational policies. These policies include complexity, life, lockout, and logging.
- Use service accounts for MSP agents and services. Disable interactive logon for these accounts.
- Restrict MSP accounts by time and/or date. Set expiration dates reflecting the end of the contract on accounts used by MSPs. Additionally, if MSP services are only required during business hours, time restrictions should also be enabled and set accordingly. Consider keeping MSP accounts disabled until they are needed and disabling them once the work is completed.
- Use a network architecture that includes account tiering. By using an account tiering structure, higher privileged accounts will never have access or be found on lower privileged layers of the network.

APT Threat Actors are actively Exploiting IT Infrastructure of Managed Service Providers and their customers

Severity: Critical

Date: October 04, 2018

RECOMMENDATIONS FOR LOGGING CONFIGURATION

- Enable all network systems and devices should have their logging features enabled. Logs should be stored both locally and centrally. Logs should also be backed up regularly and stored in a safe location.
- Ensure central log servers reside in an enclave separate from other servers and workstations. Log servers should be isolated from the internet and network environment to further protect them from compromise.
- Configure local logging servers to store log data for seven days. The default threshold for local logging should be either three days or a certain file size (e.g., 5 MB). If only size thresholds are available, NCCIC recommends that this parameter be set to a large value (e.g., 512MB to1024MB) to ensure that events requiring a high amount of log data.
- Configure central logging servers to store log data for one year. Consider increasing this capacity to two years, if possible.
- Install a SIEM appliance within the log server enclave. Configure the SIEM appliance to alert on anomalous activity identified by specific events and on significant derivations from baselined activity.
- Enable PowerShell logging. Organizations that use Microsoft PowerShell should ensure it is upgraded the latest version to use the added security of advanced logging and to ensure these logs are being captured and analyzed.
- Establish and implement a log review process. It is critical to network defense that organizations establish a regular cycle for reviewing logs and developing analytics to identify patterns.

RECOMMENDATIONS FOR VIRTUAL PRIVATE NETWORK CONNECTION

- The local network should connect to the MSP via a dedicated VPN. The VPN should use certificate-based authentication and be hosted on its own device.
- The VPN should terminate within a DMZ that is isolated from the internal network. Physical systems used within the DMZ should not be used on or for the internal network.
- Access to and from the VPN should be confined to only those networks and protocols needed for service. All other internal networks and protocols should be blocked.
- Annually update the certificates used to establish the VPN connection and consider rotating VPN authentication certificates every six months.
- All VPN connection attempts should be logged in a central location. Investigate connections using dedicated certificates to confirm they are legitimate.

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

APT Threat Actors are actively Exploiting IT Infrastructure of Managed Service Providers and their customers

Severity: Critical

Date: October 04, 2018

RECOMMENDATIONS FOR NETWORK ARCHITECTURE

- Ensure internet-facing networks reside on separate physical systems. All internet-accessible network zones (e.g., perimeter network, DMZ) should reside on their own physical systems, including the security devices used to protect the network environment.
- Separate internal networks by function, location, and risk profile. Internal networks should be segmented by function, location, and/or enterprise workgroup. All communication between networks should use Access Control Lists and security groups to implement restrictions.
- Use firewalls to protect server(s) and designated high-risk networks. Firewalls should reside at the perimeter of high-risk networks, including those hosting servers. Access to these networks should be properly restricted. Organizations should enable logging, using a centrally managed logging system.
- Configure and enable private Virtual Local Area Networks (VLANs). Enable private VLANs and group them according to system function or user workgroup.
- Implement host firewalls. In addition to the physical firewalls in place at network boundaries, hosts should also be equipped and configured with host-level firewalls to restrict communications from other workstations.

RECOMMENDATIONS FOR NETWORK SERVICE RESTRICTION

- Only permit authorized network services outbound from the internal network. Restrict outbound network traffic to only well-known web browsing services (e.g., Transmission Control Protocol [TCP]/80, TCP/443). In addition, monitor outbound traffic to ensure the ports associated with encrypted traffic are not sending unencrypted traffic.
- Ensure internal and external Domain Name System (DNS) queries are performed by dedicated servers. All systems should leverage dedicated internal DNS servers for their queries. Ensure that DNS queries for external hosts using User Datagram Protocol (UDP)/53 are permitted for only these hosts and are filtered through a DNS reputation service, and that outbound UDP/53 network traffic by all other systems is denied. Ensure that TCP/53 is not permitted by any system within the network environment. All attempts to use TCP/53 and UDP/53 should be centrally logged and investigated.
- Restrict access to unauthorized public file shares. Access to public file shares that are not used by the organization—such as Dropbox, Google Drive, and OneDrive—should be denied. Attempts to access public file share sites should be centrally logged and investigated. Recommended additional action: monitor all egress traffic for possible exfiltration of data.
- Disable or block all network services that are not required at network boundary. Only those services needed to operate should be enabled and/or authorized at network boundaries. These services are typically limited to TCP/137, TCP/139, and TCP/445. Additional services may be needed, depending on the network environment, these should be tightly controlled to only send and receive from certain whitelisted Internet Protocol addresses, if possible.

NETWORK INTELLIGENCE
Global cybersecurity provider

NEWSLETTER

September 2018, Edition 1.0

DATA BREACH HIGHLIGHTS

C&A suffers data leak in Brazil

Sept 3, 2018

The gift card platform of the retail chain has been targeted by a cyberattack.

State Department confirms breach of unclassified email system

Sept 19, 2018

The Department of State says less than 1% of employees were affected by the breach of its unclassified email system.

Inside the Magecart Breach of British Airways: How 22 Lines of Code Claimed 380,000 Victims

Sept 11, 2018

On September 6th, British Airways announced it had suffered a breach resulting in the theft of customer data.

SHEIN Data breach affected 6.42 million users

Sept 25, 2018

Another fashion retailer suffered a data breach, the victim is SHEIN that announces the security breach affected 6.42 million customers.