Health Sector Cybersecurity Coordination Center (HC3)
Sector Alert
July 10, 2020

Top 3 Malware Detections for May 2020 and Relevance to HPH Sector

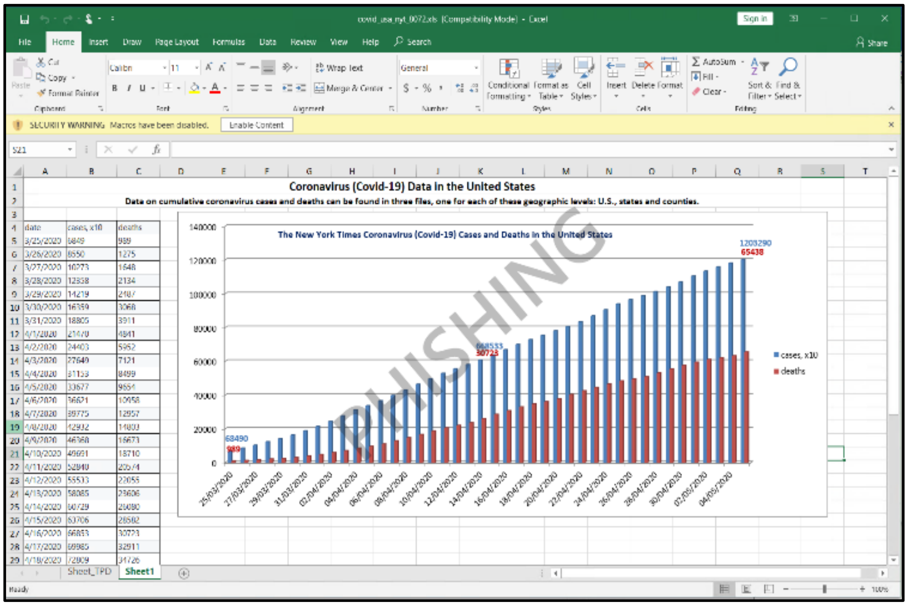
Executive Summary

Top malware detections for the month of May 2020 by the EINSTEIN national IDS included NetSupport Manager RAT, Kovter, and XMRig. According to CISA, these three threats accounted for more than 90% of active signatures. Both NetSupport Manager RAT and XMRig have links to threat actor(s) which have previously targeted the United States healthcare and public health (HPH) sector and Kovter continues to be a top malware used by threat actors. General mitigations, indicators of compromise (IOCs), techniques (TTPs), and Snort rules are provided.

Analysis

On 30 June 2020, analysts at the Cybersecurity and Infrastructure Security Agency (CISA) released the top malware detection signatures that were the most active for the month of May in the national Intrusion Detection System (IDS), known as EINSTEIN. The most prevalent malware detections involved three (3) cyber threats including: 1) NetSupport Manager RAT, 2) Kovter, and 3) XMRig.

NetSupport Manager RAT is a legitimate program that, once installed on a victim's machine, allows remote administrative control and may be used to steal information. In May 2020, Microsoft warned of an ongoing COVID-19 themed campaign, in which hackers were sending phishing emails pretending to be from the Johns Hopkins Center as an update on the number of Coronavirus-related deaths in the United States. In this massive campaign, NetSupport Manager RAT was being distributed via COVID-19 phishing emails containing malicious Excel attachments. In February 2020, hackers were found spreading a malicious Microsoft Word document disguised as a password-protected NortonLifelock document to install and deliver NetSupport Manager RAT. In the same month, another phishing campaign targeted 27 well-known companies with specially crafted emails that pretended to be from the company's vendor or client to deliver NetSupport Manager as final payload.



Coronavirus (Covid-19) Data in the United States

Data on cumulative coronavirus cases and deaths can be found in three files, one for each of these geographic levels: U.S., states and counties.

date	cases, x10	deaths
3/25/2020	6849	989
3/26/2020	8550	1275
3/27/2020	10273	1648
3/28/2020	12338	2134
3/29/2020	14219	2487
3/30/2020	16359	3068
3/31/2020	18805	3911
4/1/2020	21470	4841
4/2/2020	24403	5952
4/3/2020	27649	7121
4/4/2020	31153	8499
4/5/2020	33677	9654
4/6/2020	36621	10958
4/7/2020	39775	12957
4/8/2020	42932	14803
4/9/2020	46368	16673
4/10/2020	49691	18710
4/11/2020	52840	20574
4/12/2020	55513	22055
4/13/2020	58085	23606
4/14/2020	60729	26080
4/15/2020	63706	28502
4/16/2020	66853	30723
4/17/2020	69985	32911
4/18/2020	72809	34726

Figure 1. Microsoft detected COVID-19 themed a massive campaign starting on 12 May 2020 that distributed NetSupport Manager RAT using emails with attachments containing malicious Excel 4.0 macros. The campaign used several hundreds of unique attachments, one of which is shown above. Source: Twitter. https://twitter.com/MsftSecIntel/status/1262504864694726656/photo/1

Kovter is a constantly-evolving, fileless Trojan with several variants which initially began as a police ransomware and eventually evolved into a more effective and evasive fileless malware leveraging click fraud campaigns. While there is no direct indication that Kovter has targeted the healthcare and public health (HPH) sector from open source research, the malware continues to be a top malware recently used by threat actors according to the Center for Internet Security. In February 2017, Kovter was observed being distributed to targets in the same campaigns as Locky Ransomware. Kovter and Locky's shared distribution suggests that the threat actors behind the attacks may also be selling or renting servers as pay-per-install service.

XMRig is an open source Monero Cryptocurrency Miner that was released in May 2017 and later modified by threat actors to mine Monero cryptocurrency and has variants for CPU, NVIDIA GPU, and AMD GPU mining. XMRig can cause a victim computer to overheat and perform poorly by using additional system resources that would otherwise not be active. In October 2018, APT41, a Chinese cyber espionage group which has previously targeted the U.S. healthcare industry, compiled an instance of XMRig, a Monero cryptocurrency mining tool, demonstrating a continued interest in cryptocurrency. In June 2020, XMRig was observed targeting the Kubeflow platform on Kubernetes, an open-source container-orchestration system for automating computer application deployment, scaling, and management. Additionally, an actor known by Cisco Talos as “Vivin” has been observed distributing XMRig to indiscriminate targets meant to infect as many hosts and extract as much money as possible since as early as November 2017. Also in June 2020, the cryptocurrency mining group Tor2Mine deployed XMRig and additional malware on targeted machines during their operations to harvest credentials and steal money. In May 2020, Blue Mockingbird attackers leveraged a known vulnerability in unpatched versions of Telerik UI for ASP.NET and deployed XMRig payload in a dynamic-link library (DLL) form on Windows systems.

Alert

HC3 is sending this Alert to provide additional threat context, information, and mitigations related to NetSupport Manager RAT, Kovter, and XMRig. HC3 recommends scanning for known indicators as well as using the Snort signatures provided by CISA (included below) to detect these malware.

Patches, Mitigations & Workarounds:

CISA recommends using the following best practices to strengthen the security posture of an organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Ensure systems have the latest security updates.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' permissions to install and run unwanted software applications. Do not add users to the local administrators’ group unless required.
- Enforce a strong password policy.
- Exercise caution when opening email attachments, even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations that is configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs).
- Scan all software downloaded from the internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additionally, see the following removal guide from PCRisk for mitigations related to **NetSupport Manager RAT.**
See the Palo Alto Networks Unit 42 GitHub page for IOCs related to **NetSupport Manager RAT.**
Reference the following blog dated 7 September 2018 from Crowdstrike for remediation actions related to **Kovter**.
See the following blog post dated 24 May 2019 by Cisco Talos for IOCs and TTPs related to **Kovter**.
See the following blog post dated 21 January 2020 by Cisco Talos for IOCs related to recent Vivin **XMRig** campaigns.
The following whitepaper published 8 July 2020 by Bitdefender contains additional IOCs related to **XMRig**.

Snort Signatures

The following Snort signatures for NetSupport Manager RAT, Kovter, and XMRig were provided by the Cybersecurity and Infrastructure Security Agency (CISA) with the 30 June 2020 Alert.

1) NetSupport Manager RAT:

```
alert tcp any any -> any $HTTP_PORTS (msg:"NetSupportManager:HTTP Client Header contains 'User-Agent|3a
20|NetSupport Manager/'"; flow:established,to_server; flowbits:isnotset,.tagged; content:"User-Agent|3a
20|NetSupport Manager/"; http_header; fast_pattern:only; content:"CMD="; nocase; http_client_body;
depth:4; content:"POST"; nocase; http_method; flowbits:set,.; classtype:http-header;
reference:url,unit42.paloaltonetworks.com/cortex-xdr-detects-netsupport-manager-rat-campaign/;
reference:url,www.pentestpartners.com/security-blog/how-to-reverse-engineer-a-protocol/;
reference:url,github.com/silence-is-best/c2db;
```

2) Kovter:

```
alert tcp any any -> any $HTTP_PORTS (msg:"Kovter:HTTP URI POST to CnC Server";;
flow:established,to_server; flowbits:isnotset,.tagged; content:"POST / HTTP/1.1"; depth:15;
content:"Content-Type|3a 20|application/x-www-form-urlencoded"; http_header; depth:47; fast_pattern;
content:"User-Agent|3a 20|Mozilla/"; http_header; content:!"LOADCURRENCY"; nocase; content:!"Accept";
http_header; content:!"Referer|3a|"; http_header; content:!"Cookie|3a|"; nocase; http_header;
pcre:"/^(?:[A-Za-z0-9+\/]{4})*(?:[A-Za-z0-9+\/]{2}==|[A-Za-z0-9+\/]{3}=|[A-Za-z0-9+\/]{4})$/P";
pcre:"/User-Agent\x3a[^\r\n]+\r\nHost\x3a\x20(?:\d{1,3}\.){3}\d{1,3}\r\nContent-Length\x3a\x20[1-5][0-
9]{2,3}\r\n(?:Cache-Control|Pragma)\x3a[^\r\n]+\r\n(?:\r\n)?$/H";; classtype:nonstd-tcp;;
reference:url,www.malware-traffic-analysis.net/2017/06/29/index2.html;
```

3) XMRig:

```
alert tcp any any -> any !25 (msg:"XMRIG:Non-Std TCP Client Traffic contains JSONRPC 2.0 Config Data";;
flow:established,to_server; flowbits:isnotset; content:"|22|jsonrpc|22 3a 22|2.0|22|"; distance:0;
content:"|22|method|22 3a 22|login|22|"; distance:0; content:"|22|agent|22 3a 22|XMRig"; nocase;
distance:0; fast_pattern; content:"libuv/"; nocase; distance:0; content:!"|22|login|22 3a 22|x|22|";
flowbits:set,; classtype:nonstd-tcp;; reference:url,malware-traffic-analysis.net/2017/11/12/index.html;
reference:url,www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=1101;
```

Indicators of Compromise (IOCs)

The following are a sample of file hashes associated with NetSupport Manager RAT, Kovter, and XMRig. See linked references above in *Patches, Mitigations, & Workarounds* for additional IOCs.

1) NetSupport Manager RAT:

6e084359be25cd6372588538fa887157d741430afad547ddc14821d772577c5a
4049fd618c27031a61cc0efa703c48ed01bb93a87dbc056f4ecf48b2860ddc8d
e9440a5D2Dfe2453ae5b69a9c096f8d4cf9e059d469c5de67380d76e02dd6975
68ca2458e0db9739258ce9e22aadd2423002b2cc779033d78d6abec1db534ac2
41d27d53c5d41003bc9913476a3afd3961b561b120ee8bfde327a5f0d22a040a

2) Kovter:

0351e09f784933d3d59fe025b748e1d3fc01f545cf5dde505b034377794962c4
13d0ed2b542e6c09376adc96e9c4ef0e862727d24cbf39c6185cd8d9712c44bf
13da1a72b70ab0c78d9f1844fe5ad097e1235af32bea2f06935e32cce8e04d41
220e48a66788b6dadb06f6d326233b21694593b02140c8489dc951709a871bc1
23ae65200c6e2b11f1dfa4dc42355c2c161faa264cebe7fa62222f337a9e53f1
252de3df03b74bab9f82fe47cd809b5c3d9b86882b32a225c4abb3f9ddce955e
33d0abf301d6b4857c61e0f4d60b6a21c8ebe155731f3a737383f5f0fc055ad4
34a1ef0084d90a55ce19aa7bc0d17358247e6e3e9416b46291cb84e1b8414cef
35c9b57f3f5bffb0b1280901df5a8b4ab7fc76f453af1f72f336dad500648807
38011d4c3afaf9bb10fce05788089845a0d86edcc5424295ac3e0345d9795a59
39645016e9e74423955e24f235592ee22d48216873c6ad0abd67a57f87874af0
406a5b73c768d019808c2a779729b47d181fec402073f58ab07afc9630904198
43b3719228bb8b06e6981a2829b7920629ce1d3a650ccdf7813befe22616c3c0
57efc6fe6c36fcdac92f6210b006eac42f9ea53133f6df81a73bba822062e44d
5919b89bd4a14677da09b349d7aeeff86ba8fe690d30ce12bd55e69300393ef1
5e19b3dbc319fd8408280b4d886c9eeceffe7091151ef2b9cf5794840dd8a674
640878f3ea0254adcffe4ca564048ebe1a49a22b4821820d98a28c6f93529bc8
68f24fc9a20111bb749e1374fa1fcb832ca55f08f716561376c4aa7cc5cb60e4
6a67901c8232e4e4d9cbab3b161cd56a9c36596e92a0ad019537613f1c542ba5
6cb59a8f51d309a1b780e82c9f6e54274fdd10237dfb118fe75ce7c6d29941ec
7076e385d4b26ebaeff99786a8a5d76fedf122881d1ff29965993ee9f48bf584
730b4fade238d5afe3f535227dc729d4caf438312d6635cf65a6344ceb3888ee
74377fe4f81e47cb43780794543e5949342bb96adfb698aa80f9451a24e64b3b
7bbdad89f5b9aebe8c62048cbbc4b3f9521101ba9b25e100a3baeb24dfb1a499
7eed9a6117a9efce8a2717a695d9ccb697b0bcbd6cc85a01d530140070711945

3) XMRig:

3EA2D5E55A58309B49EADA14A007B3B8
B7070B9B317BAC578A9AC487C31879BC
3A5964C56EF16456A6B6911BEB549372

Mitre ATT&CK Tactics and Techniques

1) NetSupport Manager RAT:

ATT&CK ID	Tactic or Technique	Details
T1566.001	Phishing: Spearphishing Attachment	Malicious Microsoft Word document disguised as password-protected NortonLifelock document
T1204.002	User Execution: Malicious File	Entices user to enable macros and enter password provided in email
T1210	Exploitation of Remote Services	Install RAT to gain unauthorized access
TA0005	Defense Evasion	Employs evasion techniques to evade both dynamic and static analysis
TA0002	Execution	Utilizes the PowerShell PowerSploit framework to carry out the installation of the malicious file activity
T1036.005	Masquerading: Match Legitimate Name or Location	NetSupport Manager is a legitimate application used maliciously
T1137	Office Application Startup	Leverages winword.exe, a legitimate Microsoft Office Word process.
T1027	Obfuscated Files or Information	Leverages winword.exe to execute obfuscated batch file; obfuscates data with base64 and TripleDES encryption
T1059.003	Command and Scripting Interpreter: Windows Command Shell	Creates and executes a batch file; uses open source PowerShell script generated from PowerSploit framework to install NetSupport Manager RAT to victim machine
T1218.007	Signed Binary Proxy Execution: Msiexec	The batch script uses msiexec, which is part of the Windows Installer, to proxy execution of malicious payloads
TA0011	Command and Control	Establishes command and control with legitimate, compromised domains used by operators
TA0003	Persistence	Leverages PowerShell script to install RAT and establish persistence
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Uses registry ServiceDLL for persistence
T1518.001	Software Discovery: Security Software Discovery	Halts installation if Avast or AVG Antivirus Software is running on the target
T1543.003	Create or Modify System Process: Windows Service	Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence; the original name of NetSupport Manager is client32.exe and it was likely changed to presentationhost.exe to avoid any suspicions
T1497.003	Virtualization/Sandbox Evasion: Time Based Evasion	Sleeps for 10 seconds
T1082	System Information Discovery	Captures and sends victim computer name; retrieves geolocation of host
T1070	Indicator Removal on Host	Removes all files with extension .ps1 and deletes file named insghha4.txt
T1071.001	Application Layer Protocol: Web Protocols	Uses HTTP POST for command and control
T1313	Obfuscation or cryptography	Encrypts data sent from victim
TA0016	People Information Gathering	Phishing emails contained name of individual publicly associated with target company

Generated from: https://unit42.paloaltonetworks.com/cortex-xdr-detects-netsupport-manager-rat-campaign/

2) **Kovter:**

ATT&CK ID	Tactic or Technique	Details
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Establishes persistence in the registry of the host
T1218.005	Signed Binary Proxy Execution: Mshta	Executes the process mshta.exe
T1059.001	Command and Scripting Interpreter: PowerShell	Executes the process powershell.exe
T1218.010	Signed Binary Proxy Execution: Regsvr32	Executes the process regsvr32.exe
T1319	Obfuscate or encrypt code	Registry keys include a non-ascii character in the subkey name; registry keys contain further obfuscated javascript
T1132.001	Data Encoding: Standard Encoding	Uses base64 encoded payload, decodes it and stores it in an environment variable, again with a random name varying from infection to infection
T1543.003	Create or Modify System Process: Windows Service	Script creates a custom library function import routine to load VirtualProtect, VirtualAlloc and CreateThread from kernel32.dll as well as memset from msvcrt.dll
T1070.004	Indicator Removal on Host: File Deletion	Initial executable is deleted following infection and there are very few file system artifacts that are left behind. Powershell does not maintain a log of commands and environment variable is lost after Powershell process exits leaving little chance of recovering the script executed after the final payload.

Generated from: https://www.crowdstrike.com/blog/kovter-killer-how-to-remediate-the-apt-of-clickjacking/

3) XMRig:

ATT&CK ID	Tactic or Technique	Details
T1036.005	Masquerading: Match Legitimate Name or Location	Blue Mockingbird has masqueraded their XMRIG payload name by naming it wercplsupporte.dll after the legitimate wercplsupport.dll file.
T1543.003	Create or Modify System Process: Windows Service	Blue Mockingbird has made their XMRIG payloads persistent as a Windows Service
T1047	Windows Management Instrumentation	The file mum.txt arrives on the system as a result of the WMI event consumer script. Adversaries may abuse Windows Management Instrumentation (WMI) to achieve execution.
T1027	Obfuscated Files or Information	Mum.txt is an MZPE encrypted with a single byte XOR
TA0005	Defense Evasion	There exists different variants of XMRig to evade static detection
T1059.001	Command and Scripting Interpreter: PowerShell	Dad.txt is also a variant of XMRig, downloaded as a result of the scheduled Powershell script running periodically.
T1218.002	Signed Binary Proxy Execution: Control Panel	Downloaded from the WMI event consumer script, a very small MZPE with some exported functions generally exported by .cpl files
T1218.011	Signed Binary Proxy Execution: Rundll32	Threat actors frequently use these files because they may bypass application whitelisting and, by launching a .cpl file, Windows automatically executes them in the context of a rundll32 process launched from control.exe

Generated from: https://www.bitdefender.com/files/News/CaseStudies/study/354/Bitdefender-PR-Whitepaper-KingMiner-creat4610-en-EN-GenericUse.pdf

References

Alert (AA20-182A), EINSTEIN Data Trends – 30-day Lookback (30 June 2020)
https://www.us-cert.gov/ncas/alerts/aa20-182a
Lemos, Robert, Dark Reading, DHS Shares Data on Top Cyber Threats to Federal Agencies (1 July 2020)
https://www.darkreading.com/vulnerabilities---threats/dhs-shares-data-on-top-cyber-threats-to-federal-agencies/d/d-id/1338261
Center for Internet Security, Top 10 Malware April 2020
https://www.cisecurity.org/blog/top-10-malware-april-2020/
Unit 42, Cortex XDR™ Detects New Phishing Campaign Installing NetSupport Manager RAT (27 February 2020)
https://unit42.paloaltonetworks.com/cortex-xdr-detects-netsupport-manager-rat-campaign/
Asokan, Akshaya, BankInfoSecurity, Microsoft Warns of COVID-19 Phishing Emails Spreading RAT (22 May 2020)
https://www.bankinfosecurity.com/microsoft-warns-covid-19-phishing-emails-spreading-rat-a-14324
Meskauskas, Tomas, PCRisk, NetSupport Manager virus removal guide (19 May 2020)
https://www.pcrisk.com/removal-guides/14842-netsupport-manager-rat
Sanchez, John, Trend Micro, KOVTER: An Evolving Malware Gone Fileless (18 August 2017)
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/kovter-an-evolving-malware-gone-fileless
Proofpoint, Threat Actor Profile: KovCoreG, The Kovter Saga (1 November 2017)
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-kovcoreg-kovter-saga
Oza, Shyam, Spanning, Kovter – Malware of the Month, October 2019 (11 October 2019)
https://spanning.com/blog/kovter-malware-of-the-month/
Dubey, Sudhanshu, FireEye, Fake Software Update Abuses NetSupport Remote Access Tool (5 April 2018)
https://www.fireeye.com/blog/threat-research/2018/04/fake-software-update-abuses-netsupport-remote-access-tool.html
Cyware, A brief understanding of the XMRig Monero miner malware (11 May 2019)
https://cyware.com/news/a-brief-understanding-of-the-xmrig-monero-miner-malware-d7c05714
Varonis, Varonis Uncovers New Malware Strains and a Mysterious Web Shell During a Monero Cryptojacking Investigation (5 February 2020)
https://www.varonis.com/blog/monero-cryptominer/
Mandiant, Double Dragon: APT41, a Dual Espionage and Cyber Crime Operation (17 July 2019)
https://content.fireeye.com/apt-41/rpt-apt41/
Center for Internet Securty, Top Malware for Last Month
https://www.cisecurity.org/cybersecurity-threats/
Cyware, Phishing Attacks Now Exploit Legitimate Software for Malicious Purposes (22 May 2020)
https://cyware.com/news/phishing-attacks-now-exploit-legitimate-software-for-malicious-purposes-1489f27e/
Threatpost, Locky Ransomware, Kovter Click-Fraud Malware Spreading in Same Campaigns (3 February 2017)
https://threatpost.com/locky-ransomware-kovter-click-fraud-malware-spreading-in-same-campaigns/123560/
Unit 42, Palo Alto Networks, NetSupport Manager RAT IOCs on GitHub
https://github.com/pan-unit42/iocs/blob/master/NetSupportManager
Unit 42, Attackers Increasingly Targeting Oracle WebLogic Server Vulnerability for XMRig and Ransomware
https://unit42.paloaltonetworks.com/attackers-increasingly-targeting-oracle-weblogic-server-vulnerability-for-xmrig-and-ransomware/
BankInfoSecurity, Kubeflow Targeted in XMRig Monero Cryptomining Campaign (12 June 2020)
https://www.bankinfosecurity.com/kubeflow-targeted-in-xmrig-monero-cryptomining-campaign-a-14433
Cisco Talos, Breaking down a two-year run of Vivin's cryptominers (21 January 2020)
https://blog.talosintelligence.com/2020/01/vivin-cryptomining-campaigns.html
Cyware, XMRig Campaign Target Misconfigured Kubernetes to Mine Cryptocurrency (16 June 2020)
https://cyware.com/news/xmrig-campaign-target-misconfigured-kubernetes-to-mine-cryptocurrency-d7c60403
Security Intelligence, 'Blue Mockingbird' Attempts to Distribute Monero Miners to Enterprise Targets
https://securityintelligence.com/news/blue-mockingbird-attempts-to-distribute-monero-miners-to-enterprise-targets/
Security Boulevard, Kingminer Botnet Keeps up with the Times (8 July 2020)
https://securityboulevard.com/2020/07/kingminer-botnet-keeps-up-with-the-times/
Twitter, Microsoft Security Intelligence
https://twitter.com/MsftSecIntel/status/1262876024951328769
Twitter, Vitali Kremez @VK_Intel
https://twitter.com/VK_Intel/status/1259898696327708672