SECURONIX
Security Analytics. Delivered.

Securonix Threat Research:

CRYPTOJACKING ATTACKS - SECURONIX SECURITY ADVISORY (SSA)

Last updated: 6/13/2018

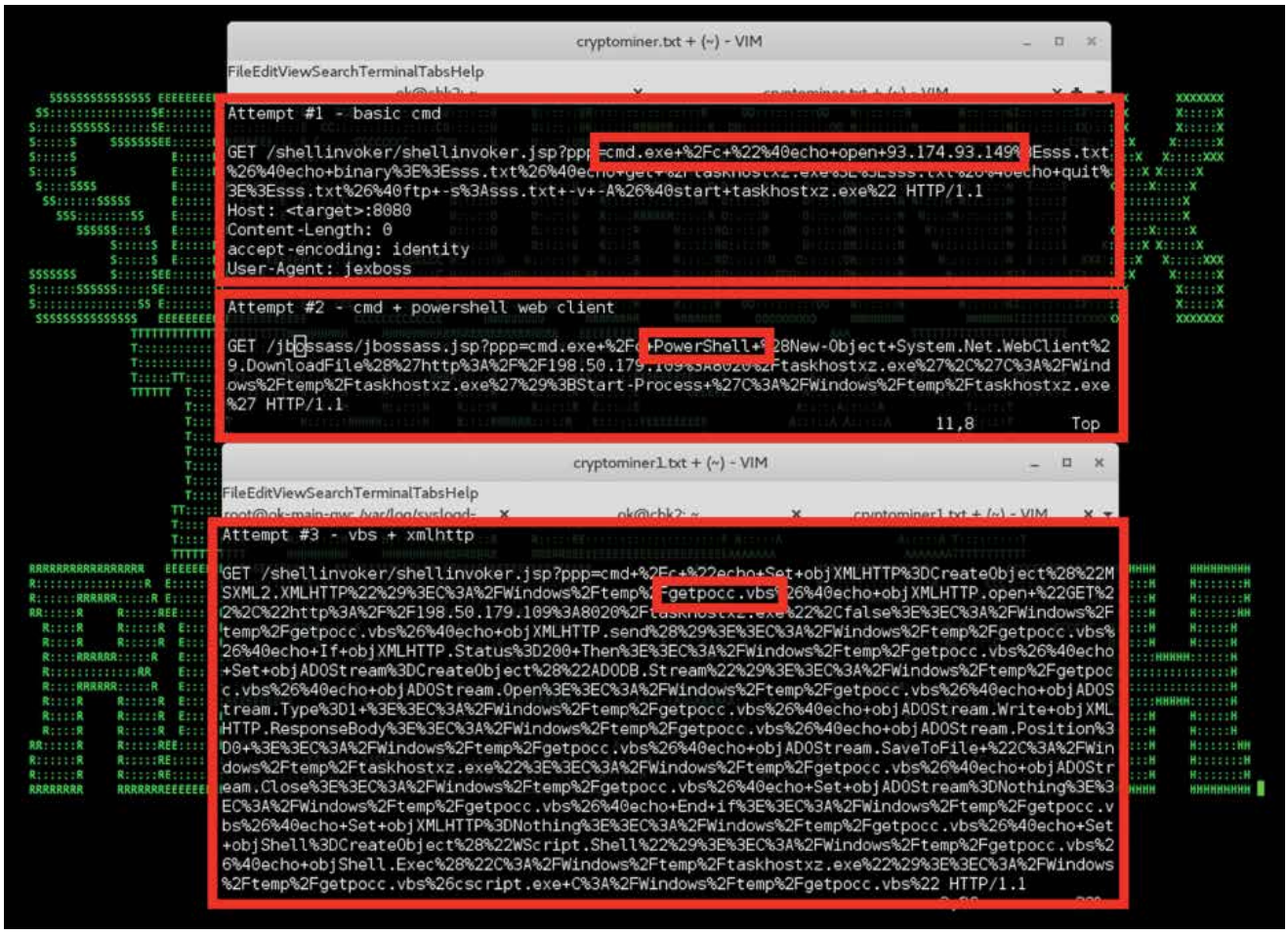

Figure 1: Persistent Cryptomining Jexboss Initial Foothold Payload - Repeated Payload Execution Attempts

Introduction

Cryptojacking is the unauthorized use of someone else's computer to secretly mine cryptocurrency (also known as virtual or digital currency). According to a recent report from Fortinet [1], Cryptojacking attacks impacted over 28 percent of companies this year, a spike representing more than 15% increase from companies impacted in the last quarter of 2017.

Securonix Threat Research Team has been actively investigating and monitoring these attacks to help our customers understand the techniques used by attackers to enable effective early detection, mitigation, and response. Below is a summary of what

we currently know about the attacks and our recommendations to help increase the chances of detecting/mitigating such attacks.

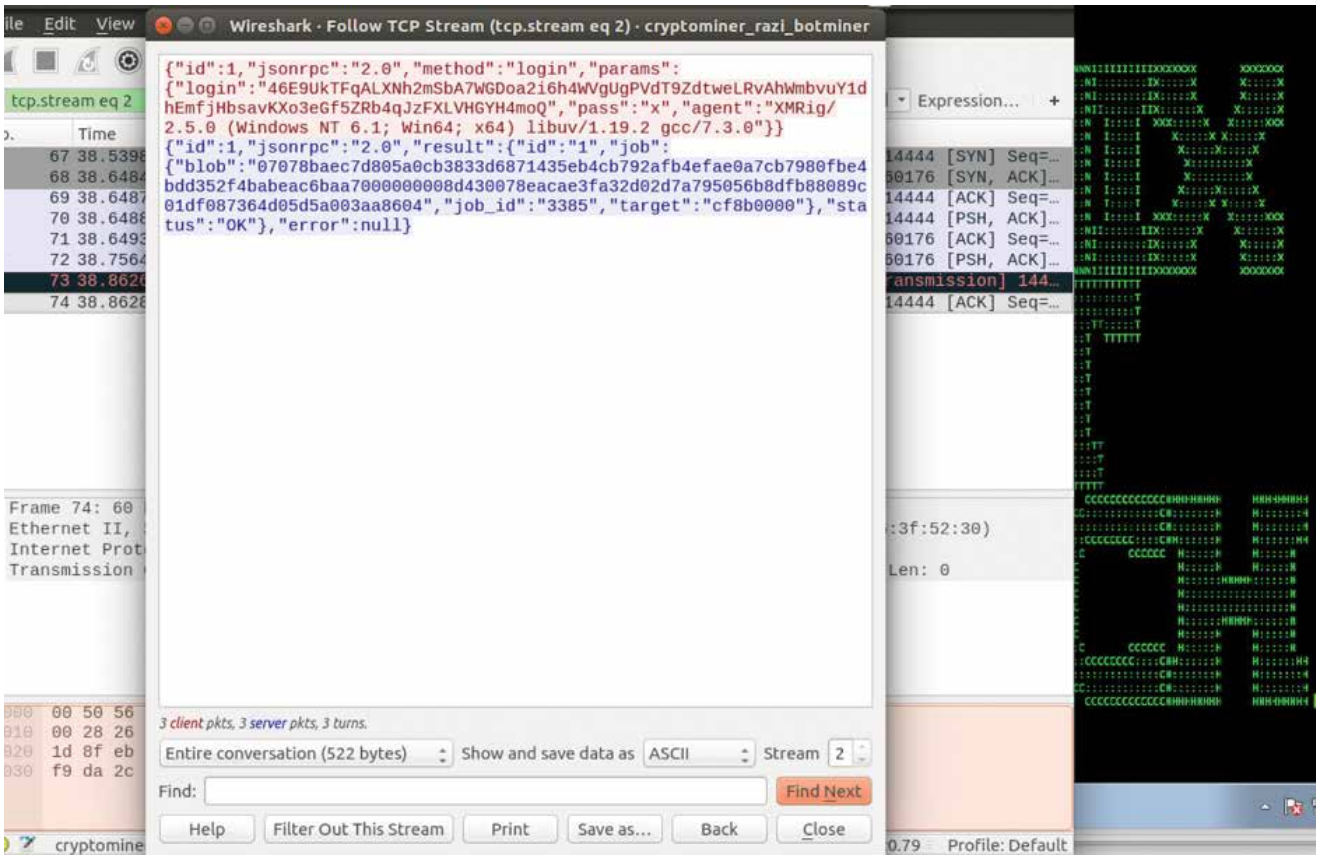

Figure 2: Cryptomining Payload Configuration Received From Command-And-Control (C2) Site

Cryptojacking Behaviors - Overview

Cryptojacking attacks are highly profitable and anonymous and can often involve not only external attackers, but also and internal rogue insider threats. The typical attack vectors used in the Cryptojacking attacks include compromising web sites [1], endpoints [2], and cloud infrastructure [3]. Some examples of the recent high-profile publicly reported breaches involving cryptojacking attacks include Los Angeles Times, Tesla, Aviva, and Gemalto [4].

As can be seen from Figure 1, modern cryptojacking attacks often involve persistent adversaries that are continuously probing infrastructure using different approaches/

payloads to inject the malicious cryptojacking payload, leveraging various attack vectors ranging from cloud misconfigurations to client-side or server-side vulnerabilities.

In most cases, the main objective of an attacker performing a cryptojacking attack is, following the initial infiltration, to quickly and secretly establish persistence that allows the attacker to run a second stage cryptomining payload continuously [6]. The configuration for the second stage cryptomining payload is usually either dynamic and downloaded from a C2 site controlled by an attacker (Figure 2), or is hardcoded in the payload.

Figure 3: Wannamine Obfuscated Malicious VBScript

Some examples of commonly used cryptomining payloads as of June 2018 include:

- xmrig
- jce
- claymore
- cpuminer
- ccminer
- minergate
- ethminer
- mkxminer
- nsgpucnminer
- sgminer
- xmr-stak
- excavator
- bminer
- minerd
- and others [5]

Based on the real-world cryptojacking activity observed by Securonix Threat Research Team in the wild, the cryptomining payloads mentioned above are often used by attackers on the exploited targets as-is. The payloads are usually renamed and set to be executed as part of a persistence mechanism available on the target, such as: a cron job, a scheduled task, a registry-based persistence, an WMI-based persistence, and other mechanisms.

In some cases, before deploying a second-stage cryptomining payload, attackers also implement a layer of obfuscation using a malicious VBScript (Figure 3) or powershell stager. The powershell stager configures the environment, checks for other cryptominer processes and shuts them down, then checks for anti-virus software.

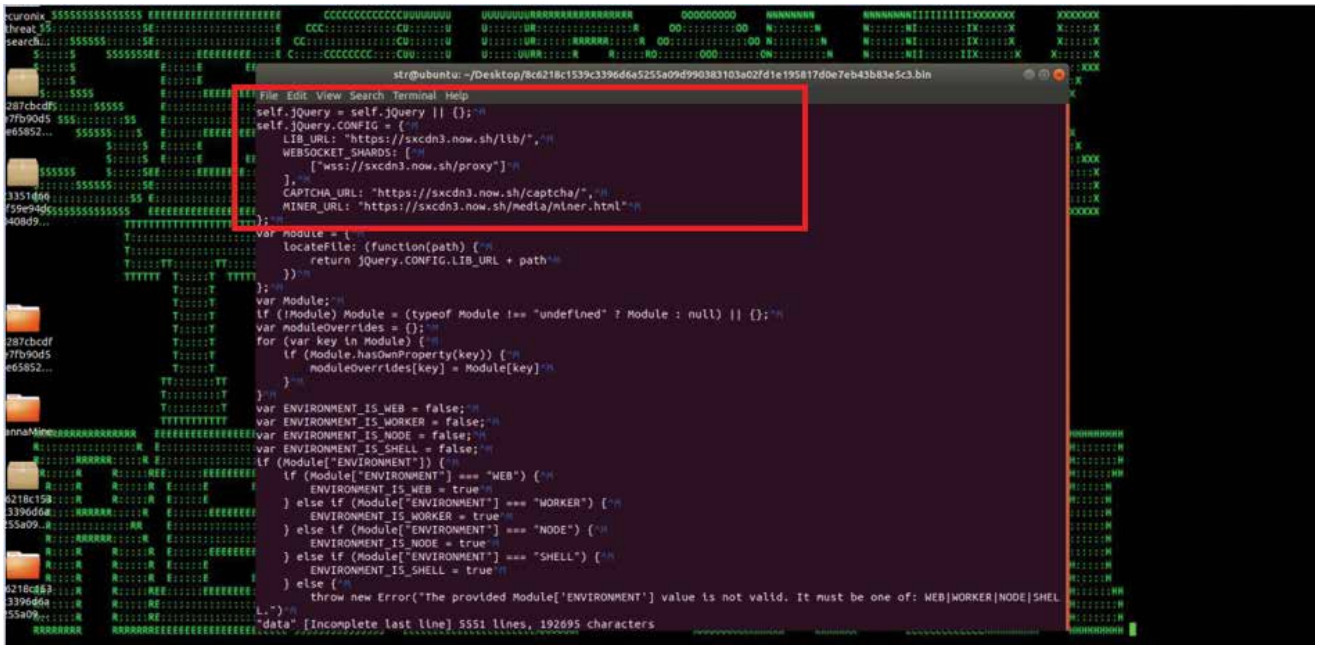

Figure 4: Javascript-Based Cryptojacking Payload [miner.ru]

Another common approach is for attackers to install a malicious cryptomining payload using a misconfigured cloud instance. This is done by injecting the payload directly into a web page and/or a third-party library loaded by a web page, which results in an end-user visiting the web page and running the cryptominer in their browser using Javascript (Figure 4).

In this case, the primary attack vector is the injection of the cryptomining script into a legitimate website. The introduction of the javascript based cryptominers, such as “CoinHive” and “Cryptoloot,” made it easier for attackers to inject the script using a link to the CoinHive or any other cryptominer tool. Attackers can then hide the script using different encoding, redirections, and obfuscation techniques.

Detection - Sample Securonix Spotter Search Queries

Below are sample Securonix Spotter search queries to assist with detecting some possible existing cryptojacking attack infections.

Endpoint Threat Detection and Response (ETDR) Process Monitoring (Trivial Process Name Conditions)

((rg_functionality=”Microsoft Windows” or rg_functionality=”Antivirus / Malware / EDR” or rg_functionality=”Endpoint Management Systems”) AND (destinationprocessname contains “xmrig” or destinationprocessname contains “minerd”or destinationprocessname contains “jce” or destinationprocessname contains “claymore” or destinationprocessname contains “cpuminer” or destinationprocessname contains “ccminer” or destinationprocessname contains “minergate” or destinationprocessname contains “ethminer” or destinationprocessname contains “mkxminer” or destinationprocessname contains “nsgpucnminer” or destinationprocessname contains “sgminer” or destinationprocessname contains “claymore” or destinationprocessname contains “xmr-stak” or destinationprocessname contains “excavator” or destinationprocessname contains “wannamine” or destinationprocessname contains “dofiol” or destinationprocessname contains “sharik” or destinationprocessname contains “coinminer”))

OR

((rg_category contains “Endpoint” OR rg_category contains “ips” OR rg_category contains “ids”) AND (sourceprocessname contains “xmrig” or sourceprocessname contains “minerd”or sourceprocessname contains “jce” or sourceprocessname contains “claymore” or sourceprocessname contains “cpuminer” or sourceprocessname contains “ccminer” or sourceprocessname contains “minergate” or sourceprocessname contains “ethminer” or sourceprocessname contains “mkxminer” or sourceprocessname contains “nsgpucnminer” or sourceprocessname contains “sgminer” or sourceprocessname contains “claymore” or sourceprocessname contains “xmr-stak” or sourceprocessname contains “excavator” or sourceprocessname contains “bminer” or sourceprocessname contains “wannmine” or sourceprocessname contains “sharik” or sourceprocessname contains “dofiol” or sourceprocessname contains “coinminer”))

ETDR Process Monitoring (Process Hash Conditions)

(rg_category contains “Endpoint” OR rg_category contains “ips” OR rg_category contains “ids”) AND (customstring3 = 57cda2f33fce912f4f5eecbc66a27fa6 or
customstring3 = 9621638daa908871e4d50a27bef014bb
customstring3 = a10157d0649cff753c01cd7bbf750608
customstring3 = 26e3021465a0a79547fbf78727b62512
customstring3 =bba538b8f6908657aeb72eaabec4a617
customstring3 =5ef3195d4676ccdec339de4ee5ded018
customstring3 =caff435e80a03dc2f21addc2d0a3b133
customstring3 =e989dc10d3d7ecebe4a2f675694b586c
customstring3 =f7f187b395aa30db56d6f432ef20d561
customstring3 =729a06f4a1a2206f1a05e15edb571771
customstring3
=1E5B11E024752C84A16B1D79E721DCE5405D72A3E2449085E33D225E4EB0E02E
customstring3
=CCF801F123A895871E5B937092244DF15C943DC288BA6D8490648C7D682A6FFA
customstring3 =3a6dd15bce3818fe00a79c202f8a7561
customstring3 =a6ce06ce8ffb132127eac19b79480ba4ed09e828
customstring3 =4d2dd2a5b66b91d3660ce400ced0ef1f
customstring3 =337651740c627345a73c08fd571a830bb6b7983a
customstring3 =d08177f271cef298725f434cc6d31230
customstring3 =718057117639d74b6470a3d754d5d1109b7e78db
customstring3 =fe90bc53a44b7627f38edc87e24d7334
customstring3 =8d2c7359f24450ada709736a653c1ca52ea1d3d5
customstring3 =b3112199f173e17cc48cf09dc309115e
customstring3 =02cb05880e4d543175643a41f860f0da42b80a56
customstring3 =f638a308dacd22eeff2126a332412887

customstring3 =935a3bcf68fa452f8ea8149bf116775aa2a89005
customstring3 =0b8391a640fd4069fd03274b9dc37334
customstring3 =f6c284b19aebb08834cc5d35611d06bcf3ba2419
customstring3 =a9ba518aae14c1690dcc7a4c29d8d561
customstring3 =95007634471d7fdd35fbade7bf75b234ef1c09f4
customstring3 =2c798cce7e85edfe64e5a4e450729ec8
customstring3 =797b9ad1123594abe3dd48f85dccc52438e33c67
customstring3 =d2a4d1247752fb186841ff4c2985341b
customstring3 =7aa259b88e8bfd27d033bed11ca30d3c1a2c35aa
customstring3 =90116f06b905abe01a601f06416e839e
customstring3 =90c9d49b565308ec0bdc172a1e35bc72757860bf
customstring3 =511664d75e23d1b7c7a85615df65b121
customstring3 =3b6d0940fa19225bd35b91fa5563d1916dac7b97
customstring3 =cc30bbba9dfa6c13fc64c54497870279
customstring3 =35c41b6ff826ab999298765e5b423ca8afec0b82
customstring3 =260ebc182b267a1b5db70193e70c7d8a
customstring3 =1f380ab82e97370cb5ebaf59cca40a563a7e8339
customstring3 =4603d077153e4013042bdb4d2b392fba
customstring3 =66d5eb0091a24e7c13596e5e70efdf0d5e88abec
customstring3 =de8e252012047320d79ead835701d6dc
customstring3 =c9994a5d786c1e597f7030fcb7312fd049d14dc8
customstring3 =28662e5424a5b825752429e3837bc7a8
customstring3 =89525352d2cd4de249dd199ea5ab209d1d2f756e
customstring3 =b5df5a71499c0404a997b2039961b3ad
customstring3 =627c4b8a83b70a0a670aeb1466332d875686ecdc
customstring3 =4db0c33744bdc72fdf35ecc5f0297010
customstring3 =6a3b664eaf9ad476467b04ed3a04f10226df1e54

customstring3 =3f2a23b919ab1bc37bdb0866a4a5ce77
customstring3 =9285217c217da6556d1a1254a793c16b3c4108ff
customstring3 =b7127fb068465a6f3992311d2045e023
customstring3 =c5166ff8bfb896b6c0af1a654bbb7a42db7df286
customstring3 =3fb53ce2f7af70b03041bda852e14675
customstring3 =c4c6ed79d4dfff04dd42c4a90a411f19767b8eb6
customstring3 =c67024788bf53c050eb139e55917d682
customstring3 =659503484be2a5cdc2fc06ef51726fa3ab118d95
customstring3 =5cf8d2a6b894863ce1c25c864235e4e0
customstring3 =ad43829aea685ad1a587661d4e3f640db2da5538
customstring3 =ec31f0d5935213377c8792b2e9fb0d07
customstring3 =ad6b9e62a7ea132e1bec0efd8d9e5f8a2ae531ca
customstring3 =e4118b01e3dd93d6129d8b535dadd90b
customstring3 =8327546d971b1a09b5cac2e6ef664e676ed90611
customstring3 =5ab01b2bcaf87576fb51a2fa6a802cf1
customstring3 =a26bc03a779669166701be2f184c3bd69cb678a0
customstring3 =aa9f5203c3380fa5bbd2b27744695bac
customstring3 =1e2ce9ec27e1121e92ed4bb1e8df8e9cafe7c549
customstring3 =54e6aa961ebfb28b9d0149bd63f75ebe
customstring3 =6d8fe648343280fef2b4f52072567d518deb4cc5
customstring3 =9ce5eb167c745716471f1c6d1a51a028
customstring3 =bbdab3f21bbce114d972045b9056c64f299ef7a7
customstring3 =0e661f023e66b5e7b455306178322b94
customstring3 =b2b6e218bdf989530d4246d82c345e92bbb0f7b3
customstring3 =dad2d0a48b97c9f411eaf8bf8c182ba3
customstring3 =701ab83d693a06622ec594f1148be38dc679c1c5
customstring3 =db849eb62868a4f56c9c8f67bdbae9ee
customstring3 =2bbc59939d8d4de805136c74a87787ed61326bfa
customstring3 =6fb295138ad278ee9db8497d7e11a03a
customstring3 =cf218f1244f7a64c021701b3766bcc172a3d0499)

Mitigation and Prevention - Securonix Recommendations

This section provides recommendations from Securonix to help customers mitigate and prevent attacks:

1. Implement a company-wide coinblocker URL and IP Block list/blackholing in your firewall using the following: https://gitlab.com/ZeroDot1/CoinBlockerLists/issues/1

2. Implement a user security policy requiring the use of a browser extension to block cryptomining such as Nocoin: (https://chrome.google.com/webstore/detail/no-coin-block-miners-on-t/gojamcfopckidlocpkbelmpjcgmbgjcl?hl=en) or MinerBlock (https://chrome.google.com/webstore/detail/minerblock/emikbbbebcdfohonlaifafnoanocnebl) Note: Firefox 63 update (releases in October 2018) is scheduled to add protection against cryptomining websites.

3. Review the third-party components used by your company's websites and add protection from third-party js library component cryptojacker injection by leveraging subresource integrity (SRI) and content security policy (CSP) tags such as crossorigin, integrity, require-sri-for etc.: <script src="https://scotthelme.co.uk/js/jquery2.1.3.min.js" noncanonical-src="https://ajax.googleapis.com/ajax/libs/jquery/2.1.3/jquery.min.js" integrity="sha256-ivk71nXhz9nsyFDoYoGf2sbjrR9ddh+XDkCcfZxjvcM=" crossorigin="anonymous"></script> Note: See https://scotthelme.co.uk/subresource-integrity/ and https://scotthelme.co.uk/content-security-policy-an-introduction/)

4. Perform a review of the cloud storage sites (e.g. Amazon S3 buckets) used to deliver content for your company's web sites for unusual changes related to potential cryptojacking modules. Also, consider an external review of the web components used by your organization for possible cryptojacking modules using PublicWWW: https://publicwww.com/websites/%22coin-hive.com%2Flib%2Fcoinhive.min.js%22+site%3Acom/.

5. Review the types of instances used as part of your cloud infrastructure for instance types that may be unusual, such as Amazon Accelerated Computing/GPU instances (P3, P2, F1, *.xlarge, see https://aws.amazon.com/ec2/instance-types/).

Securonix Detection – Some Examples of Securonix Predictive Indicators

1.1 Recommended Data Sources

Below is a list of the recommended data sources to help you cover some of the key behaviors used in cryptojacking attacks:

1. EDR: Endpoint logs such as Bit9/Carbonblack or sysmon, and auditd for container/ docker infrastructure logs.

2. PXY: Proxy logs

3. CLO: Cloud services activity and performance/resource utilization logs such as Amazon AWS, CloudTrail/CloudWatch/Macie, EC2, IAM, S3 Access, Microsoft Azure, Google Cloud, and container logs (Docker/Kubernetes).

4. IFW: Firewall logs

5. OCU: Other/custom logs, particularly those related to performance monitoring of your infrastructure (e.g. *beats, Tanium*)

1.2 Examples of Relevant High-Level Behavior Analytics/Predictive Indicators

This section provides high-level examples of Securonix behavior analytics/predictive indicators based on some of the key attack vectors used in the latest cryptojacking attacks impacting endpoints and cloud infrastructure:

- Suspicious Process Activity - Rare Parent-Child Relationship For Host Analytic
- Suspicious Process Activity - Targeted - Executable File Creation Analytic
- Suspicious Network Activity – Rare Outbound Network Connection For Host Analytic
- Suspicious Cloud Activity - Rare StartInstances/TerminateInstances Source Analytic
- Suspicious Process Activity - Rare Scheduled Task For Host Analytic
- Suspicious WMI Activity - Rare WMI Consumer For Host Analytic
- Suspicious Windows Activity - Unusual CPU Utilization Amount For Host Analytic

Other behavioral analytics/predictive indicators include: EDR-SYM6-ERI, EDR-SYM5-ERI, WEL-PSH-BPI, PXY-IPB1-TPN, EDR-SYM15-ERI, EDR-SYM35-BAI, EDR-SYM34-BPI, CLO-AWS10-BDI, WEL-WOT1-RUN, EDR-SYM25-RUN, WEL-WSH1-ERI, WEL-TAN1-BAI, WEL-TAN2-BPI, EDR-SYM36-BPI, and EDR-SYM37-ERI.

Note: It is important to keep in mind that there are many other attack vectors and log sources/data sources that need to be considered depending on the potential attack surface/infrastructure, such as web server, application, and container system logs.

References

[1] Fortinet Threat Landscape Report - Q1 2018. April, 2018. https://www.fortinet.com/fortiguard/threat-intelligence/threat-landscape.html. Last accessed: 6-2-2018.

[2] Lily Hay Newman. Hack Brief: Hackers Enlisted Tesla's Public Cloud To Mine Cryptocurrency.February 20, 2018. https://www.wired.com/story/cryptojacking-tesla-amazon-cloud/. Last accessed: 6-2-2018.

[3] Kelly Sheridan. 25% of Businesses Targeted with Cryptojacking in the Cloud. May 15, 2018. https://www.darkreading.com/cloud/25–of-businesses-targeted-with-cryptojacking-in-the-cloud/d/d-id/1331813. Last accessed: 6-2-2018.

[4] Lindsey O'Donnell. Cryptojacking Attack Found On Los Angeles Times Website. February 22, 2018. https://threatpost.com/cryptojacking-attack-found-on-los-angeles-times-website/130041/. Last accessed: 6-2-2018.

[5] koinshieldeditor. Mining Program MD5 & SHA1. February 22, 2018. https://koinshield.com/2018/02/22/mining-application-hashes/. Last accessed: 6-2-2018.

[6] FireEye. CryptoMiners: An Overview of Techniques Used Post-Exploitation and Pre-Mining. February 15, 2018. https://www.fireeye.com/blog/threat-research/2018/02/cve-2017-10271-used-to-deliver-cryptominers.html. Last accessed: 6-8-2018.

SECURONIX

ABOUT SECURONIX

Securonix is radically transforming all areas of data security with actionable security intelligence. Our purpose-built, advanced security analytics technology mines, enriches, analyzes, scores and visualizes customer data into actionable intelligence on the highest risk threats from within and outside their environment. Using signature-less anomaly detection techniques that track users, account and system behavior, Securonix is able to detect the most advanced insider threats, data security and fraud attacks automatically and accurately.

CONTACT SECURONIX

www.securonix.com
info@securonix.com | (310) 641-1000

0618


SECURONIX
Security Analytics. Delivered.