# A Rare Look Inside a Cryptojacking Campaign and its Profit

intezer.com/blog/research/a-rare-look-inside-a-cryptojacking-campaign-and-its-profit/

January 13, 2021



#### Written by Nicole Fishbein - 13 January 2021



#### **Get Free Account**

#### Join Now

#### Intro

Linux threats are becoming more frequent. A common type of Linux threat is **cryptojacking**, which is the unauthorized use of an IT system for the purpose of mining cryptocurrency. While cryptominers are well-documented, it's not often that you get an inside look. It's rare to see the dashboard of the wallets being used in an active cryptojacking campaign with dozens of victims, as well as the attacker's profit margin.

This post details an ongoing cryptojacking campaign targeting Linux machines, using <u>exposed Docker API ports</u> as an initial access vector to a victim's machine. The attacker then installs a Golang binary, which is undetected in VirusTotal at the time of this writing.

The file serves as a Monero cryptominer installer and sets up configuration for the miner. The attack uses SSH to maintain superiority on the victim's machine, leaving a backdoor and installing its own SSH keys on the host.

This campaign has been active for nearly a year. We are certain that each day at least one payment is passed into two wallets and there are currently 95 workers. Workers are victim machines whose resources are being used to mine cryptocurrency for the attacker. A snapshot of the active workers is shown in Figure 1.

						H
•	•	•	••	• •	· · · ·	Found 25 Min Age
Rece	wa 👻 🧃 43Y5gWFUZmCS93jkY5V4Q	A86to5wy	AWMbZUdPYtiG7EF8ZKk4uA3BAj1eMoTns8whP3Eo	eaVdy55L1wcBkKn894kUpdimMq		0.02562449
	1			36.4 KH/s Ang 8 Hrs		
	95 Workers		3,499,472,995	.234 53.	696,565 / 11,482	0.0449 XMR
	3 Sec Aga		Total Hashes	,,	Valid / Invalid Sharea	S6.5 NU(s 💙 Per Day 💙
	172.18.14.219		43-c58480584-0048-1225061_27480 1.8 KH/s		bi2019_23402 1.3 KH/s	c7-compute1_14016 479 H/s
	daping	792 H/s	twr_27741 521 H/s	db_14372 583 H/s		host-101-132-221-202_30826 2 KH/s
	i-eamojifsn_30393	1.2 KH/s	1015-160_31286 979 H/s		lb-worker-1.bfv.tw.de_5716 1.6 KH/s	moniliang_3925 ** 1.3 KH/s
	nextclass-Node-service-mgr2_16575				NiceHash_0102_2829 1.6 KH/s	NiceHash_0102_4111 986 H/s
	NiceHash_0102_4203				NiceHash_0105_2866 396 H/s	NiceHash_0105_3879 604 H/s
	NiceHash_0108_3514				NiceHash_0109_1225 521 H/s	NiceHash_0109_1343 396 H/s
	Man MAN AN A	1-11-				0 - 00 - 00 - 0 - 00

Figure 1: Snapshot of workers mining cryptocurrency for the attacker

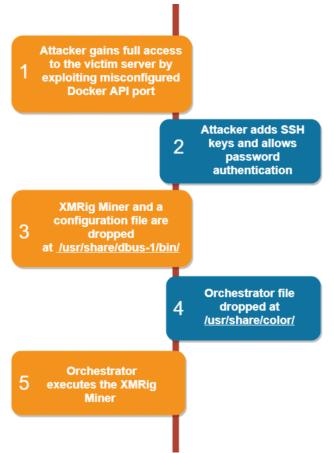
### **Attack Flow**

A new attack flow takes advantage of a known Docker misconfiguration, putting the host at risk for being compromised. The attacker exploits this misconfiguration to gain full control over the Docker daemon and creates a new container with access to the host's filesystem. With access to the filesystem, the attacker installs malware on the Docker host.

First, the attacker establishes a stable SSH connection by adding their own SSH key to the host and editing the configuration of the SSH service to allow password authentication. These modifications remove dependency on the misconfiguration, giving the attacker a stable connection to the victim.

Next, they install two binary files on the host: an XMRig Miner at location /usr/share/dbus-1/bin/ and an orchestrator file at /usr/share/color/. We analyzed this file and came to the conclusion that it's being used to execute XMRig Miner and to ensure it keeps running.

The orchestrator is responsible for preparing and initializing configurations for the execution of the coinminer malware. Before running the coinminer, it verifies the path /usr/share/dbus-1/bin contains two files: systemd-host (aka the miner) and the other named **IBus**, the miner's configuration file.



#### Figure 2: The attack flow

The path **/usr/share** is not commonly seen in Linux malware and is writable only with root privileges. The path **/tmp** is more often seen as an installation path in Linux malware since it does not require root privileges. The attacker has root privileges because the container they escaped from has them and hence the attacker has access to /usr. Placing the files at /usr may imply that they are taking advantage of the high privileges they have in order to use this path as some sort of hiding technique that is harder to detect.

The configuration file reveals interesting insights about the miner and the attack campaign. From the configuration we can tell that the target cryptocurrency is Monero, known to be more private than other coins like Bitcoin. This means that the details of the transaction amounts and the sender/recipient identities are disguised. In addition, we found the address of the pools and the IDs of two wallets used in this campaign. The address of the pools belongs to <u>supportxmr</u> domain and the wallets are still active at the time of this publication.

### Take a Look (or Two) at the Dashboards

It's rare to find an active wallet with victim information for a few reasons. Management of the wallets is taken care of by another server that acts like a proxy so that the malware connects without providing the wallet. In some cases, the wallets are not active or have only a few workers. In this recent attack, we found a live dashboard—shown in Figure 3— that is constantly updated with new workers and paints the full picture of this campaign.

T 🖇 XMR								Home 👻 🤇
O	°000 ° °	••	• •	· · · ·	•.		•. •. •. •.	Found 8 Min Age
Reo	sent 👻 🤠 43Y5gWFUZmC59JjkY5V4Q	A86to5wyA	WMbZUdPYtiG7EF82Kk4uA3BAj1eMoTns8whl	9EoeaVdy55L1wcBkKn894kUpdimMq			0.05366064 view 32.957	
	the gas to the second space	any ti		Bis S KH/s Avg 8 Hrs )				
	74 Workers		3,343,459,	678.351	51.2	34,762 / 9,439	0.0460 XMR	
	3 Sec Ago		Total Har			alid / Invalid Shares	B6.2 NAUs ♥ Per Day ♥	
0	172.18.14.219			KH/s appwar			/s c7-compute1_14016 697 H/s	0
	daping			H/s ecs-5ad2_27699			/s i-eamqifsn_30393 2 KH/s	
	icns-160_31486	mi	imm	KH/s izbp16f13hkhqcf1hlxbpqz_31467			/s jiaxy-precision-tower-3620_12615 1.9 KH/s	
	lb-worker-1.bfv.tw.de_5716			KH/s nextclass-Node-service-mgr2_1657			/s NiceHash_1209_249 979 H/s	
	NiceHash_1211_1936			H/s NiceHash_1212_1214			/s NiceHash_1212_2101 915 H/s	
	NiceHash_1212_2210			KH/s NiceHash_1212_3186			/s NiceHash_1212_4575 2.1 KH/s	
	NiceHash 1212 534	646 H/s	NiceHash 1212 550 33	H/s NiceHash 1215 1714	1.8 KH/s	NiceHash 1215 3144 625 H	/s NiceHash 1215 4086 729 H/s	

Figure 3: Screenshot of the first mining dashboard

The dashboard shows that this campaign has been active for almost a year with both wallets receiving at least one payment per day. One of the wallets averages 95 workers while the second wallet averages four workers, meaning the campaign is still operational and has about 100 victims to date.

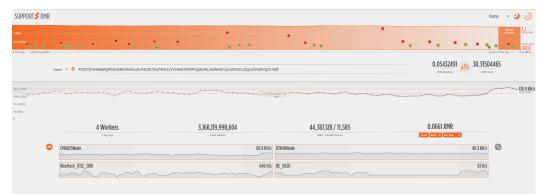


Figure 4: Screenshot of the second mining dashboard

## **Insights About the Victims**

172.18.14.219 812 H/s	43-c58480584-0048-1225061_27480 1.6 KH/s	annwar 604 H/s	bi2019_23402 1.4 KH/s	c7-computel 14016 500 H/s
				ip-172-31-20-154 17480 795 H/s
				nextclass-Node-service-mgr2 16575 667 H/s
				NiceHash 1212 1105 2 KH/s
				NiceHash 1212 2210 2.1 KH/s
	NiceHash_1212_3186 729 H/s		NiceHash_1212_3928 958 H/s	NiceHash_1212_4575 2.4 KH/s
				NiceHash_1215_2663 222 H/s
have mene	hand		man	momment
NiceHash_1215_3144 562 H/s	NiceHash_1215_4086 166 H/s	NiceHash_1215_746 1.8 KH/s		NiceHash_1216_4635 646 H/s
m	man		······································	mmmm
			NiceHash_1217_2206 250 H/s	NiceHash_1217_2452 798 H/s
Mann	man			
NiceHash_1217_2956 1.9 KH/s	NiceHash_1217_3528 166 H/s	Node_12409 1.7 KH/s	Node_9126 625 H/s	Nodegpu_2065 2 KH/s
~~~~		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	mmmmm	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Nodeserver 2287 3.7 KH/s	Nodeserverazon 27153 2.1 KH/s	ns31169008 8404 671 H/s	ns3137774_14314 1.1 KH/s	op-benchmark-202 2.1 KH/s
mmmm	m	mont	mmmm	mmmmm
op-benchmark-203 17761 1.8 KH/s	op-benchmark-210 1.4 KH/s	op-benchmark-211 479 H/s	op-benchmark-213 1.4 KH/s	op-benchmark-215 229 H/s
man	mmmmm	mmmm	man	mmmmm

Figure 5: Screenshot of the active workers, their names and hash rates

CPU 🗍	H/s 🔻	TDP \$	APP 👙	PARAM	\$ os	ŧ	DATE 븆	<\$ ≑
4X AMD OPTERON 6348 - <u>Buy Now</u>	10612	N/A	RandomX Benchmark Linux x64.	seq 0 7   xargs -p 0 -i node numactl -n node ./randomx-benchmark minelargepagesjitnonces 100000init 6threads 6	OTHER LINUX OS x64		Jul, 2019	\$
RYZEN 3900X Buy Now	10503	165 W	RandomX Benchmark Linux x64.	minethreads 30init 24nonces 800000largepagesjit	UBUNTU 18.04 x64		Jul, 2019	4
4X XEON E5-4640	10500	380 W	XMRig 4.4.0 beta (rx/0)	N/A	OTHER LINUX OS x64		Oct, 2019	4
AMD RYZEN THREADRIPPER 2920X - Buy Now	10500	105 W	XMRig 6.3.5-mol	CPU@default with 4*16GB DDR4 RAM@3200MHz	WINDOWS 10 x64		Oct, 2020	4
RYZEN 7 3700X - Buy Now	10262	167 W	XMRig 6.4.0-dev. SOURCE: MGUR	3700X @ 4.1 GHz, G.Skill Trident Z RGB (2x16GB) @ 3600 MHz 14-14-14-28 with tuned sub-timings: $\rm \underline{IMGUR}$	WINDOWS 10 x64		Oct, 2020	4

#### Figure 6: Screenshot from Monero benchmarks

Using the randomx CPU benchmarks, we can cross-reference the hash rates seen in the dashboard (Figure 4) with the CPU type that generates them as shown in Figure 5. From this comparison we can see that most of the victims are not machines with high levels of performance but rather standard hosts similar to your home computer. But if we examine the rates from the wallet that has only three workers, we can infer its workers have more computing resources than those in the other wallet given their CPU power.

It's possible that the attacker uses different wallets to separate high and low performance victims.

We examined the workers' names. Some of them contain a string that looks like a date, which we assume is the date of infection. In Figure 6, for example, the marked numbers can be translated into 01/11, or January 11.



Figure 7: Screenshot from the dashboard disclosing the name of the worker

### **Mitigation**

#### **Fix your Misconfigured Docker API Port**

Misconfiguration of the Docker API port is one of the most common yet deadly mistakes users can make. Fortunately, this cryptomining operation can be easily avoided just by having a secure configuration. <u>Download our How-To Guide</u> to configure your Docker API ports in 4 simple steps.

### **Docker Security Best Practices**

This article provides a <u>checklist of Docker security best practices</u>, from development and deployment onto the production environment. In addition, you can verify that other misconfigurations do not pose a risk to your environment via lateral movement by referencing this <u>list of Docker misconfigurations</u>.

### **Integer Protect Community Edition**

Advanced attacks like SolarWinds and Pay2KEY have shown that focusing only on vulnerabilities in your own code is not enough to secure your environment. It's time to assume breach and detect and respond to attacks when they occur in production.

<u>Integer Protect</u> is a Cloud Workload Protection Platform designed to protect Linux machines in runtime against unauthorized code. With Integer Protect you can easily detect cryptominers and other threats in your cloud, as well as identify the misconfiguration that could have been exploited—in this case, in Docker. <u>Try our free community edition</u>.

Executing the orchestrator file will prompt an immediate alert in Intezer Protect as seen in Figure 8.

📦 INTEZER PROTECT	🔿 Dashboard	🗥 Alerts	{I} Code	Assets	Add Asset				Docs Research Pr	rotect - Enterprise Ready 📀
< Back to Alerts										
Severe X M								Created on: 10 Jan 21   15:05 PM		Close Alert ×
🗏 Asset Deta	ils					🗅 File Deta	ails			
Sensor status: Hostname: Distribution: OS Version: OS Release:	☆ Connected ubuntu-test-env Ubuntu 18.04.4 [7 Linux #30-18.04; 5.3.0-28-generic						: 13 Dec 20   2	18:29 PM 3709cc08b036a895280f33b7a8650d7b000107bafd5bd0cb lysis		
<b>থ All Executi</b>	ons									
Running proces	s tree									
	temd/systemd /lib/systemd/system						X Malicious Exec Execution Time: PID: Path:	ution PID: 39387 13 Dec 20   13:51 PM 39387 /usr/chare/color/systemd-host		
	78   /usr/lib/gnome							/usr/share/color/systemd-host 39386 0		
	PID: 39386   /usr							0 pts0 Running Terminate Process ©		
										(?) Help

Figure 8: Execution of the orchestrator captured in Intezer Protect

When XMRig Miner is executed by the first file, Intezer Protect will trigger a second alert as seen in Figure 9.

📦 INTEZER PROTECT				Add Asset				
< Back to Alerts Severe A malicious file has be		File I xmr						Close Alert X
🗏 Asset Deta	ils				🗅 File Det	tails		
Sensor status: Hostname: Distribution: OS Version: OS Release:	☆ Connected ubuntu-test-env Ubuntu 18.04.4 L Linux #30-18.04, 5.3.0-28-generic					e: 13 Dec 20   In: 2 ■ 15 Dec 20   13.67 MB	18:29 PM ce5aae311e906b8311a1975f8c1431b83618f3d11aeaff10ae lysis	
양 All Executi	ons							
Running proces	s tree							
PID: 1   /lib/sys								
	/lib/systemd/syster						13 Dec 20   13:42 PM 39150 /usr/share/dbus-1/bin/systemd-host	
		e-terminal/gnome-te						
							39146 1000 1000	
							pts0	
							Running Terminate Process 🛇	() Help

Figure 9: Intezer Protect alert triggered upon the execution of XMRig Miner

intezer protect	Alerts (1) Code	Assets Add Asset			Docs Roy Halevi
< Back to Assets					
docker-ho	st				
● Infected   😤 Conr					
Hostname: docker-host	Platform: 💩 AWS Instance ID: i-04a98dc29				
Asset Details Confi	guration Checks				
Search					
Vulnerability status			Check number		
High					
Description: Rationale: Remediation:	By default, the Docker daemon binds to a non-n could have full access to the Docker daemon and	tworked Unix socket and runs with root p therefore in turn to the host system. For or the daemon and for any Docker Swarn als.	- orivileges. If you change the default Docker daem this reason, you should not bind the Docker dae	ess to the Docker daemon via IP address and port. on binding to a TCP port or any other Unit socket, anyone with a mon to another IP/port or a Unix socket. If you must expose the C ion restricts the connections to your Docker daemon over the net	ocker daemon via a network
Medium					
Medium	Ensure permissions on /etc/shadow- are configur	d	6.1.7	Linux CIS	(?) Help

Figure 10: Intezer Protect reports on Docker misconfiguration with an open API port

#### The Bottom Line

The threat described in this post is an example of a well-detected miner that uses SSH to maintain connection with the victim; but also leaves a "trail" that privies us to information we rarely get to see from a cryptojacking campaign.

Cryptomining malware has become a familiar threat on Linux servers because it's relatively cheap and easy to launch. It's not often that you get to see how profitable these campaigns can be for the attacker—with access to the wallets, how much they earned and the dashboard as the attacker sees it.

### loCs

### **XMRig Miner**

240fe01d9fcce5aae311e906b8311a1975f8c1431b83618f3d11aeaff10aede3

### Miner\_installer

8ecffbd4a0c3709cc98b036a895289f33b7a8650d7b000107bafd5bd0cb04db3

### Wallets' Addresses

43Y5gWFUZmCS9JjkY5V4QA86to5wyAWMbZUdPYtiG7EF8ZKk4uA3BAj1eMoTns8whPJEoeaVdy55L1wcBkKn894kUpdimMq (mining pool: <u>https://supportxmr.com/</u>)

49XZTjHS4aNjWgPhxbWNnDhiKnuJL4YKdE7JEyf45U1yYYe9ebTiS9PPUg8yJEL26eNHECyLH2DnUCuDgoZhhdiFVgD19kP (mining pool: <u>https://supportxmr.com/</u>)

49r6Mp1fcb4fUT5FPTgaz9E47fZV7n6JiY76c4vdBZvgDm8GmWHTVYM9Azpe4MsA9oXs2RpUNPPfH7oXABr3QnwNQKaP2W7 (mining pool: <u>https://supportxmr.com/</u>)

43Xbgtym2GZWBk87XiYbCpTKGPBTxYZZWi44SWrkqqvzPZV6Pfmjv3UHR6FDwvPgePJyv9N5PepeajfmKp1X71EW7jx4Tpze (mining pool: <u>https://xmr.nanopool.org</u>)

82etS8QzVhqdiL6LMbb85BdEC3KgJeRGT3X1F3DQBnJa2tzgBJ54bn4aNDjuWDtpygBsRqcfGRK4gbbw3xUy3oJv7TwpUG4 (mining pool: <u>https://www.f2pool.com</u>)

47PXdhiZphNHka2K1J9udPj5Nct4zpvCRUMqwVY4Rvyxf3FLmPqyR6J68hDX4fUF65jNxJa43szPM3Ni5zDerArzSkdFp1K (mining pool: <u>https://supportxmr.com/</u>)

47xS7CWWZ8c7xdxBcuiqA7KLK8kRFcaLFPViKA9w3eHVe2WcKj8iaBEADzZYXGqE9sCC71cbu64qrZhZZkafzFn2VPA9xs9 (mining pool: <u>https://minexmr.com/</u>)



#### **Nicole Fishbein**

Nicole is a malware analyst and reverse engineer. Prior to Intezer she was an embedded researcher in the Israel Defense Forces (IDF) Intelligence Corps.