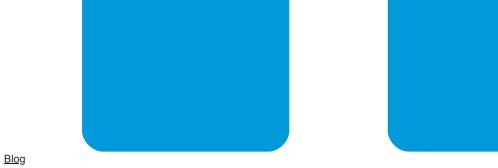
Smominru Monero mining botnet making millions for operators

proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators





<u>Threat Insight</u> Smominru Monero mining botnet making millions for operators



```
January 31, 2018 Kafeine
```

Overview

Even with recent volatility in the price of most cryptocurrencies, especially Bitcoin, interest among mainstream users and the media remains high. At the same time, Bitcoin alternatives like Monero and Ethereum continue their overall upward trend in value (Figure 1), putting them squarely in the crosshairs of threat actors looking for quick profits and anonymous transactions. Because obtaining these cryptocurrencies through legitimate mining mechanisms is quite resource-intensive, cybercriminals are <u>stealing them</u>, demanding ransomware payments in them, and <u>harnessing other computers</u> to mine them for free. Recently, Proofpoint researchers have been tracking the massive Smominru botnet, the combined computing power of which has earned millions of dollars for its operators.

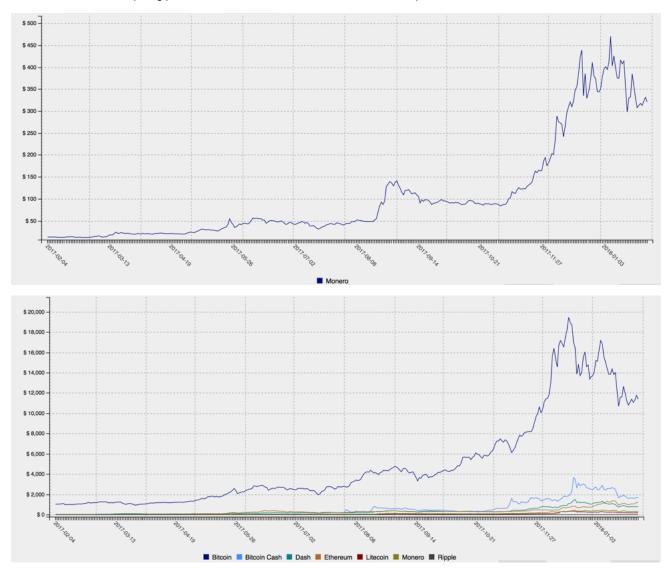


Figure 1: Monero cryptocurrency values (top) and relative values of major cryptocurrencies, including Bitcoin, over the past year (bottom)

Analysis

Since the end of May 2017, we have been monitoring a Monero miner that spreads using the EternalBlue Exploit (CVE-2017-0144). The miner itself, known as Smominru (aka Ismo [6]) has been well-documented [1] [2] [3] [4] [5] [10], so we will not discuss its post-infection behavior. However, the miner's use of Windows Management Infrastructure is unusual among coin mining malware.

The speed at which mining operations conduct mathematical operations to unlock new units of cryptocurrency is referred to as "hash power". Based on the hash power associated with the Monero payment address for this operation, it appeared that this botnet was likely twice the size of Adylkuzz [9]. The operators had already mined approximately 8,900 Monero (valued this week between \$2.8M and \$3.6M). Each day, the botnet mined roughly 24 Monero, worth an average of \$8,500 this week (Figure 2).

Your Stats & Payment History

Look at worker stats for hash rates and worker stats

45bbP2muiJHD8Fd5tZyPAfC2RsajyEcsRVVMZ7Tm5qJjdTMprexz6yQ5DVQ1BbmjkMYm9nMid2QSbiGLvvfau7At5V18FzQ	

Address: 45bbP2muiJHD8Fd5tZyPAfC2RsajyEcsRVVMZ7Tm5qJjdTMprexz6yQ5DVQ1BbmjkMYm9nMid2QSbiGLvvfau7At5V18FzQ

Pending Balance: 8.663820939590 XMR

🏛 Personal Threshold (Editable): < 0.500 XMR >

Once you reach your threshold, you will get a free auto-payout within 24 hours

Manual Payments Disabled

Total Paid: 6590.147446270000 XMR

! The following stats are only for the base address and not all workers:

O Last Share Submitted: less than a minute ago

Hash Rate: 3.33 MH/sec

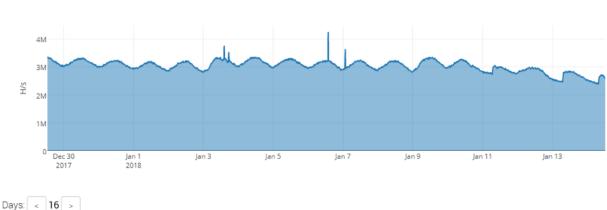
Total Hashes Submitted: 38274200548984

Sent Payments:

⊘ Time Sent	Transaction Hash	🖸 Amount	📥 Mixin	Fee
08/01/2018, 01:48:44	4daac13abd5630249ca73318ff3fabc0e212468d0bd3b22b0500d54552be7250	24.8158	5	0.000
07/01/2018, 01:47:42	c8a79ccbc52751d03425f370f0f7d9f61b1de7818a1831822e000893cc667abb	27.9581	5	0.000
06/01/2018, 01:46:34	f9b436f79cde7d29ce2b538b2fc18f618d3d958ed0c2f2444b2b9a7cdd1f6006	21.8523	5	0.000
05/01/2018, 01:45:41	f3ad82cf7358d2378977f03b9bf77778941c73520483367536cf97b135297dab	24.7673	5	0.000
04/01/2018, 01:44:16	bfeeffe66a8eed2ffae2974d2ae290307350f8210362c382d36460c320eaaae2	24.1817	5	0.000

Figure 2: Smominru Stats and Payments on the MineXMR mining pool

We could also see that the average hash rate to date this year was quite high (Figure 3):



Total hashrate history

🍘 Average Total Hash Rate: (24h) 2.61 MH/s (12h) 2.53 MH/s (1h) 2.62 MH/s (10m) 2.70 MH/s

Figure 3: Smominru hash rate history on MineXMR

At least 25 hosts were conducting attacks via EternalBlue (<u>CVE-2017-0144</u> SMB) to infect new nodes and increase the size of the botnet. The hosts all appear to sit behind the network autonomous system AS63199. Other researchers also reported attacks via SQL Server [3], and we believe the actors are also likely using EsteemAudit (<u>CVE-2017-0176</u> RDP), like most other EternalBlue attackers. The botnet's command and control (C&C) infrastructure is hosted behind SharkTech, who we notified of the abuse but did not receive a reply.

With the help of abuse.ch [7] and the ShadowServer Foundation [8], we conducted a sinkholing operation to determine the botnet size and location of the individual nodes. The botnet includes more than 526,000 infected Windows hosts, most of which we believe are servers. These nodes are distributed worldwide but we observed the highest numbers in Russia, India, and Taiwan (Figures 4 and 5).

Q Lookup

Smominru Country Distribution

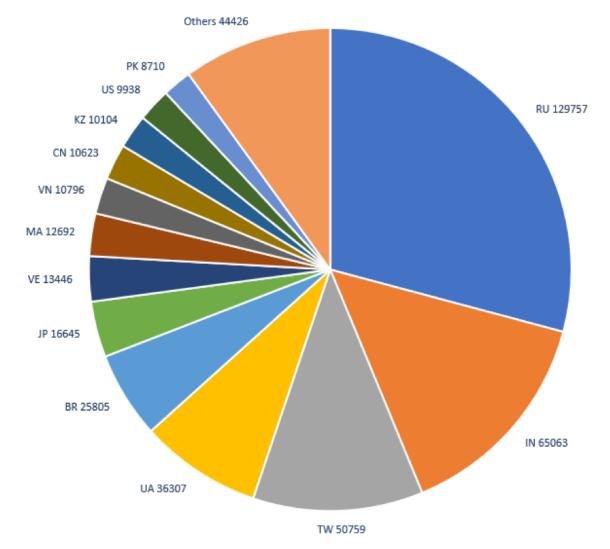


Figure 4: Geographic distribution of Smominru nodes

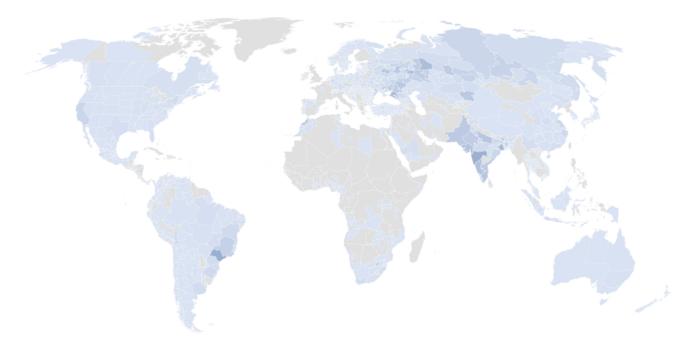


Figure 5: Concentration of Smominru nodes worldwide

We contacted MineXMR to request that the current Monero address associated with Smominru be banned. The mining pool reacted several days after the beginning of the operation, after which we observed the botnet operators registering new domains and mining to a new address on the same pool. It appears that the group may have lost control over one third of the botnet in the process (Figure 6).



```
Days: < 11 >
```

🍘 Average Total Hash Rate: (24h) 1.79 MH/s (12h) 1.61 MH/s (1h) 1.70 MH/s (10m) 1.69 MH/s

Per Worker Stats

Getting Started with Worker IDs

note: only 1000 worker IDs per address are supported

🚯 Hash Rate	✓ Accepted Shares	 Expired Shares 	Invalid Shares	O Last Share Submitted	Worker ID
1.69 MH/s	1786162957834	8797261723	72918228	less than a minute ago	43LYBd

Accepted Shares: These are valid shares, and your payout is calculated based upon these.

Expired Shares: These are shares which were submitted too late for the current block. It is normal for this to be less than 1% of your accepted shares.

Invalid Shares: These are shares submitted which provide an incorrect hash. You should aim for this to be 0. Common causes are unstable overclocks.

Figure 6: Smominru adapting to the sinkholing and returning to two thirds of its hash rate with a new Monero mining address

Your Stats & Payment History

Look at worker stats for hash rates and worker stats

4	3Lm9q14s7GhMLpUsiXY3MH6G67Sn81B5DqmN46u8WnBXNvJmC6FwH3ZMwAmkEB1nHSrujgthFPQeQCFPCwwE7m7TpspYBd	Q Lookup
a,	Address: 43Lm9q14s7GhMLpUsiXY3MH6G67Sn81B5DqmN46u8WnBXNvJmC6FwH3ZMwAmkEB1nHSrujgthFPQeQCFPCwwE7m7TpspYBd	
Î	Pending Balance: 5.968969158884 XMR	

Personal Threshold (Editable): < 4.200 XMR >

Once you reach your threshold, you will get a free auto-payout within 24 hours

Manual Payments Request Payment (0.004XMR Fee) Disable Manual Payments

Total Paid: 98.891429595000 XMR

! The following stats are only for the base address and not all workers:

Last Share Submitted: less than a minute ago

Hash Rate: 2.03 MH/sec

Total Hashes Submitted: 1432059315308

Sent Payments:

⊘ Time Sent	📽 Transaction Hash	Amount	📥 Mixin	Fee
23/01/2018, 02:01:51	6d54e29e83d19e3cfee8523311936b84f04b06d87c90d469b0458c89445da9d3	12.3298	5	0.000
22/01/2018, 02:01:20	b33227db1cf25ccffd9d3cfd3fe5920fd6675db69b9547b6e25011a69e8d57c1	13.2615	5	0.000
21/01/2018, 02:00:30	d90364985e573b9bcd6b89692ef3c5180f8d3e0ceb4218ebf8baf12db1083dd9	13.1020	5	0.000
20/01/2018, 01:59:32	fea24bc754bceb2aba2e4d93c839d685942417910104ff962bcfc4a88016fe91	12.5457	5	0.000
19/01/2018, 01:59:02	caabd8e7bd0077673f7d8a1c879bbd997fe33dea570b97b4be5e5b1d2e8fc02b	14.3028	5	0.000
18/01/2018, 01:58:26	5df84a19162d3bddf817e09d65bf6f664a03f339411bd20a04d03354d3c12a18	14.8672	5	0.000
17/01/2018, 01:57:24	502b2238258ee3f244d6026c6d17f0140d833620cda4f405527aae5b80033e37	12.8203	5	0.000
16/01/2018, 01:55:45	05449a601d26212993bec0e7ad3744270d784028ef9bfdf6471eed22b8e69fdf	5.6621	5	0.000

Figure 7: Smominru statistics and payments associated with their new mining address

Conclusion

Cryptocurrencies have been used by cybercriminals for years in underground markets, but in the last year, we have observed standalone coin miners and coin mining modules in existing malware proliferate rapidly. As Bitcoin has become prohibitively resource-intensive to mine outside of dedicated mining farms, interest in Monero has increased dramatically. While Monero can no longer be mined effectively on desktop computers, a distributed botnet like that described here can prove quite lucrative for its operators.

Because most of the nodes in this botnet appear to be Windows servers, the performance impact on potentially critical business infrastructure may be high, as can the cost of increased energy usage by servers running much closer to capacity. The operators of this botnet are persistent, use all available exploits to expand their botnet, and have found multiple ways to recover after sinkhole operations. Given the significant profits available to the botnet operators and the resilience of the botnet and its infrastructure, we expect these activities to continue, along with their potential impacts on infected nodes. We also expect botnets like that described here to become more common and to continue growing in size.

Acknowledgement

We would like to thank abuse.ch and ShadowServer for their help.

References

[1] https://securelist.com/blog/research/77621/newish-mirai-spreader-poses-new-risks/

- [2] http://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-miner-uses-wmi-eternalblue-spread-filelessly/
- [3] https://www.guardicore.com/2017/12/beware-the-hex-men/ (Taylor)
- [4] https://blogs.yahoo.co.jp/fireflyframer/34858380.html

[5] https://www.77169.com/html/158742.html	
[6] https://www.reddit.com/r/antivirus/comments/6maxrt/tenacious_malware_called_ismolsmo/	
[7] <u>https://abuse.ch/</u>	
[8] https://www.shadowserver.org/	
[9] https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue- doublepulsar	
[10] http://blog.netlab.360.com/mykings-the-botnet-behind-multiple-active-spreading-botnets/	
Indicators of Compromise (IOCs)	
IOC	ІОС Туре
down.oo000oo[.club:8888 209.58.186[.]145	domain:p
www.cyg2016[.xyz:8888 103.95.29[.]8	domain:p
	·
down.mys2016[.info:8888 103.95.29[.]8	domain:p
wmi.mykings.top[.info:8888 45.58.140[.]194	domain:p
	p
wmi.oo000oo[.club:8888 45.58.140[.]194	domain:p
xmr.5b6b7b[.ru:8888 45.58.140[.]194	domain:p
64.myxmr[.pw:8888 170.178.171[.]162	domain:p
wmi.my0709[.xyz:8888 103.95.30[.]26	domain:p
ftp.ruisgood[.ru:21 68.64.166[.]82	domain:p
ftp.oo000oo[.me:21 68.64.166[.]82	domain:p
ftp.ftp0118[.info:21 68.64.166[.]82	domain:p
js.mys2016[.info:280 27.255.79[.]151	domain:p
J3.113920 T0[.1110.200 27.200.70[.]10 T	uomain.p

down.my0709[.xyz 103.95.30[.]26	domain:p
down.my0115[.ru:8888 103.95.30[.]26	domain:p
wmi.my0115[.ru:8888 103.95.30[.]26	domain:p
js.my0115[.ru:8888]	domain:p
Xmr.xmr5b[.ru:8888] 45.58.140[.]194	domain:p
64.mymyxmra[.ru:8888] 170.178.171[.]162	domain:p
Down.down0116[.info] 198.148.80[.]194	domain II
67.229.144[.218:8888]/ups.rar	URI
198.148.80[.194:8888]/0114.rar	URI
103.95.30[.26:8888]/close2.bat	URI
www.pubyun[.com]/dyndns/getip	URI
xmr.5b6b7b[.ru:8888]/xmrok.txt	URI
64.myxmr[.pw:8888]/cudart32_65.dll	URI
64.myxmr[.pw:8888]/md5.txt	URI
down.my0709[.xyz:8888]/ok.txt	URI
wmi.my0709[.xyz:8888]/test.html	URI
da3b2e4da23aae505bf991cb68833d01d0c5b75645d246dfa9b6e403be1798c8	sha256
8ceb370e5f32dd732809c827f8eda38cc9b746d40adea3dca33b8c27ee38eb6f	sha256
5e15c97546a19759a8397e51e98a2d8168e6e27aff4dc518220459ed3184e4e2	sha256
2e3f534bd6b7d1cf18dc727820124faed92fb28f1d4626c9658587b9b3c09509	sha256

7f8b5cb8fc7bd5c14105fde118f5ac7a808e590e52f16c70128b4bd28aa4b5a	sha256
2e0712ff24e5f9ab8ee682a53514c501486f0836ef24125503335d86bd10a4e	sha256
o1824b41f3853376e21153d9125781dbb57b820d8a9a6cc037f82ea87f50973	sha256
c36aebdcd92a04fd689d31944e5388e7e9b9421063ec4c98804ac7a04e6b0d	sha256
5bbP2muiJHD8Fd5tZyPAfC2RsajyEcsRVVMZ7Tm5qJjdTMprexz6yQ5DVQ1BbmjkMYm9nMid2QSbiGLvvfau7At5V18FzQ	Monero Address
7Tscy1QuJn1fxHiBRjWFtgHmvqkW71YZCQL33LeunfH4rsGEHx5UGTPdfXNJtMMATMz8bmaykGVuDFGWP3KyufBSdzxBb2	Monero Address
3Lm9q14s7GhMLpUsiXY3MH6G67Sn81B5DqmN46u8WnBXNvJmC6FwH3ZMwAmkEB1nHSrujgthFPQeQCFPCwwE7m7TpspYBd	Monero Address
48.153.34[.]114	IP
18.193.81[.]70	IP
18.193.31[.]14	IP
18.193.28[.]58	IP
64.52.12[.]110	IP

164.52.13[.]58

148.153.38[.]78

118.193.22[.]58

IP

IP

IP

103.241.229[.]122	IP
148.153.39[.]186	IP
148.153.14[.]246	IP
118.193.31[.]110	IP
118.193.27[.]198	IP
164.52.25[.]106	IP
164.52.1[.]46	IP
148.153.36[.]34	IP
118.193.21[.]186	IP
164.52.12[.]162	IP
148.153.24[.]106	IP
148.153.44[.]46	IP
164.52.11[.]222	IP
118.193.29[.]6	IP
148.153.8[.]86	IP
164.52.1[.]14	IP
ET and ETPRO Suricata/Snort Signatures	
2829231 ETPRO TROJAN Win32/Smominru Coinminer Checkin	
2804781 ETPRO POLICY DynDNS IP Check getip	
2018959 ET POLICY PE EXE or DLL Windows file download HTTP	
2015744 ET INFO EXE IsDebuggerPresent (Used in Malware Anti-Debugging)	
2022886 II ET POLICY Crypto Coin Miner Login	

2022886 || ET POLICY Crypto Coin Miner Login

2024789 || ET POLICY DNS request for Monero mining pool

2829329 || ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2018-01-17 1)

Subscribe to the Proofpoint Blog