Money-making machine: Monero-mining malware

welivesecurity.com/2017/09/28/monero-money-mining-malware/

September 28, 2017

While far behind Bitcoin in market capitalization, Monero has several features that make it a very attractive cryptocurrency to be mined by malware.

While the world is holding its breath, wondering where notorious cybercriminal groups like Lazarus or Telebots will strike next with another destructive malware such as WannaCryptor or Petya, there are many other, less aggressive, much stealthier and often very profitable operations going on.

One such operation has been going on since at least May 2017, with attackers infecting unpatched Windows webservers with a malicious cryptocurrency miner. The goal: use the servers' computing power to mine Monero (XMR), one of the newer cryptocurrency alternatives to Bitcoin.

To achieve this, attackers modified legitimate open source Monero mining software and exploited a known vulnerability in Microsoft IIS 6.0 to covertly install the miner on unpatched servers. Over the course of three months, the crooks behind the campaign have created a botnet of several hundred infected servers and made over USD 63,000 worth of Monero.

ESET customers are protected against any attempts to exploit the CVE-2017-7269 vulnerability, even if their machines aren't patched against it, as was the case with EternalBlue, the exploit used to spread WannaCryptor.

Why mine Monero and not Bitcoin?

While far behind Bitcoin in market capitalization, Monero has several features that make it a very attractive cryptocurrency to be mined by malware – untraceable transactions and a proof of work algorithm called CryptoNight, which favors computer or server CPUs and GPUs, in contrast to specialized mining hardware needed for Bitcoin mining.

We can observe the exchange rate jumping up from 40 USD/XMR up to 150 USD/XMR over the past month, falling back to 100 USD/XMR.

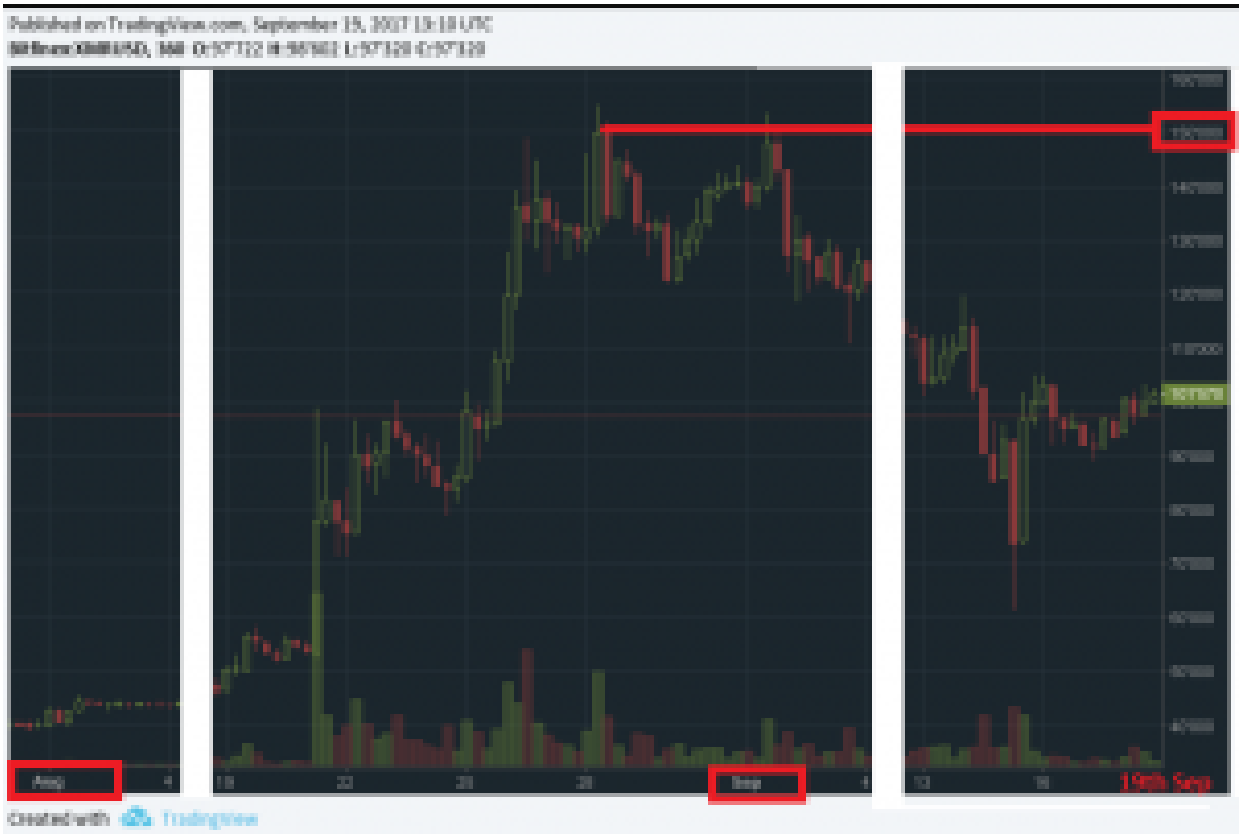

Figure1. Candlestick chart of the XMR/USD exchange rate in August, 2017

The Cryptominer

First seen in-the-wild on 26th May, 2017, the malicious mining software is a fork of a legitimate open source Monero CPU miner called xmrig, version 0.8.2 (also released May 26 2017).

When creating the malicious mining software, the crooks did not apply any changes to the original open source codebase apart from adding hardcoded command line arguments of the attacker's wallet address and the mining pool URL, plus a few arguments to kill all previously running instances of itself so as not to compete with its new instance. This couldn't have taken the cybercrooks more than just couple of minutes as suggested by the fact that we saw it in-the-wild on the same day the base version of xmrig was released.

You can see the attacker's modified cryptominer and its identification with the available source code in the figures below.

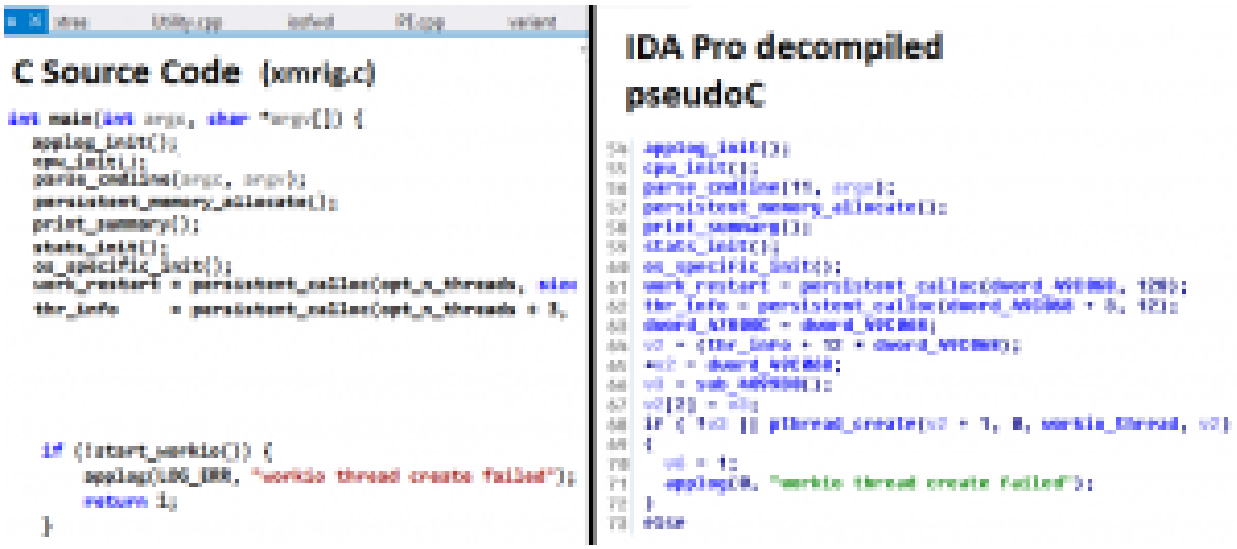

Figure2. Code comparison between original and adapted versions

Scanning and Exploitation

The distribution of the miner to victims' computers is the hardest part of this operation, but even here, the attackers went for the easiest approach. There are two IP addresses that we identified as the source of brute-force scans for the CVE-2017-7269 vulnerability and both point to servers in the Amazon Web Services cloud.

The vulnerability exploited by the attackers was discovered in March 2017 by Zhiniang Peng and Chen Wu. It is a vulnerability in the WebDAV service that is part of Microsoft IIS version 6.0, the webserver in Windows Server 2003 R2. A dangerous buffer overflow in the ScStoragePathFromUrl function is triggered when the vulnerable server is processing a malicious HTTP request. In particular, a specifically crafted PROPFIND request leads to a buffer overflow due to a reallocation of double sized buffer when the count of Unicode characters is mistakenly provided instead of a byte-count. A very detailed analysis of the mechanism by Javier M. Mellid can be found here. This vulnerability is especially susceptible to exploitation, since it's located in a webserver service, which in most cases is meant to be visible from the internet and therefore can be easily accessed and exploited by anyone.

The payload comes necessarily in the form of an alphanumeric string. The attackers replaced the string leading to the execution of the Windows calculator from the proof-of-concept with one leading to the download and execution of their malicious payload. However, this didn't require much sophistication either, as there are online tools like alpha3 that help to convert any shellcode into the desired string.

The shellcode is the expected download-and-execute action (downloading *dasHost.exe* from hxxt://postgre[.]tk/ into the %TEMP% folder):

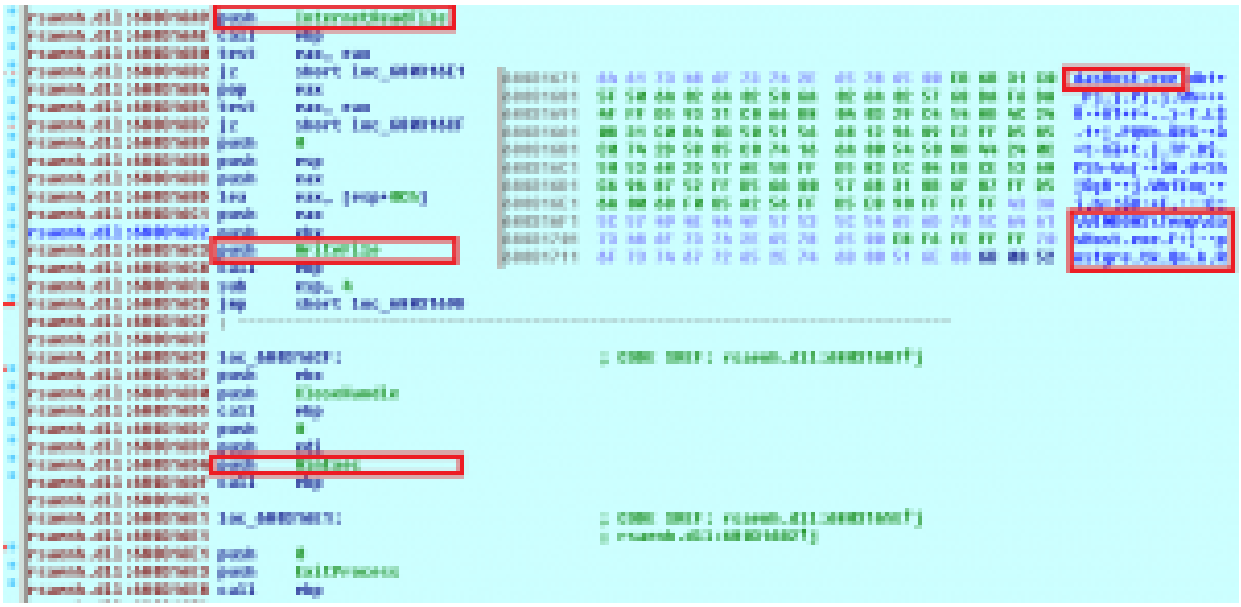

Figure3. Shellcode delivered by the exploit

Based on our data, the very first in-the-wild exploitation of this vulnerability happened just two days after its publication on 26th March 2017 and it has been actively exploited ever since.

This particular malicious miner was first seen in-the-wild on 26th May 2017. Since then, it has been appearing in waves, on a weekly or less frequent basis, which implies that the attacker scans the internet for vulnerable machines.

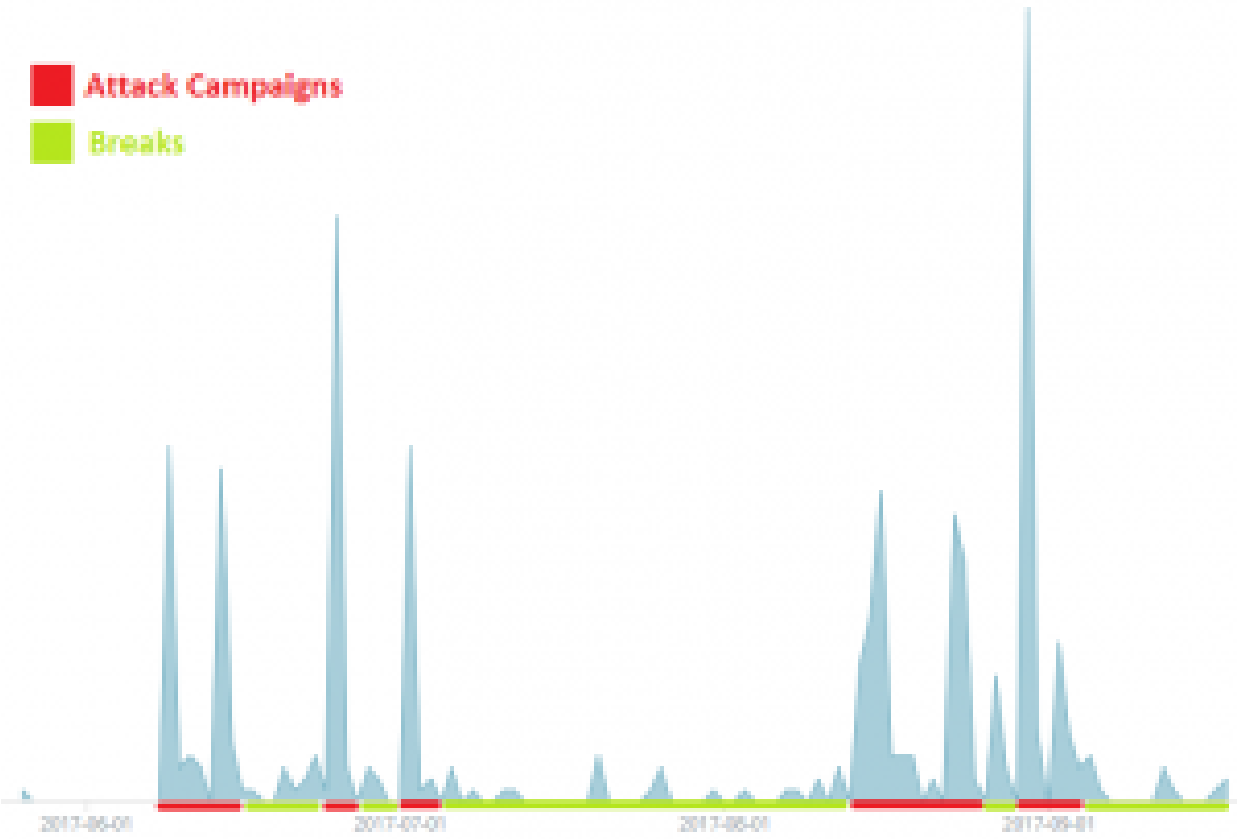

Figure4. Graph of infection waves over time

Scanning is always done from one IP address, which seems to be a machine hosted on an Amazon cloud server that the attacker had rented and deployed their scanning software, and continue to use it to launch their attacks.

Mitigation

ESET detects the malicious binaries of the miner as **Win32/CoinMiner.AMW trojan** and the exploitation attempts at the network layer under the detection name **webDAV/ExplodingCan**. This is a real-world example of a packet that would be blocked:

Figure5. Specifically crafted HTTP request with an encoded shellcode

Microsoft ended its regular update support for Windows Server 2003 in July 2015 and did not release any patch for this vulnerability until June 2017, when several critical vulnerabilities for its older systems were discovered and brought to the attention of malware authors. The good news is that despite the end-of-life status of the system, Microsoft decided to patch these critical vulnerabilities in order to avoid large-scale destructive attacks similar to the WannaCryptor (aka WannaCry) outbreak. However, keeping Windows Server 2003 up-to-date might be difficult due to the fact that automatic updates don't always work smoothly (e.g. this blog post by Clint Boessen confirms our own troubles with updating the system). Consequently, many of these systems are still vulnerable to this day. We strongly advise users of Windows Server 2003 to apply KB3197835 and other critical patches as soon as possible (if automatic updates fail then download and install the security update manually!).

Statistics

Thanks to the mining pool stats being publicly available, we were able to see the combined hash rate of all victims, which represents the computing power dedicated to the mining account. The value seemed to consistently reach around 100 kilohashes per second (kH/s), with a surge of up to 160 kH/s in late August 2017, which we attribute to campaigns launched on August 23 and 30.

Overall, the infected machines were making approximately XMR5.5 daily by the end of August and have made over XMR420 in total over the course of three months. According to the exchange rate of 150 USD/XMR at the time, these values were equal to USD 825 per day and over USD 63,000 in total, respectively.

The attackers were very active at the end of August but have gone quiet since early this month with no new infections coming in. Moreover, because the miner has no persistence mechanism, the attackers have slowly begun losing already compromised machines, and the total hash rate has dropped all the way down to 60 kH/s at the time of writing. This is not the first time the attackers took such a break and it is likely a new campaign will be launched in the near future.

The total number of victims is not known to us, but can be estimated from the total hash rate produced by the attacker. According to the CPU benchmarks, a high-end consumer Intel i7 processor has a hash rate of around 0.3-0.4 kH/s. However, considering the fact that the exploit is limited to systems running Windows Server 2003, which will most likely be running on older hardware with weaker CPUs, the average hash rate per victim will be much lower and the total number of infected machines probably much higher.

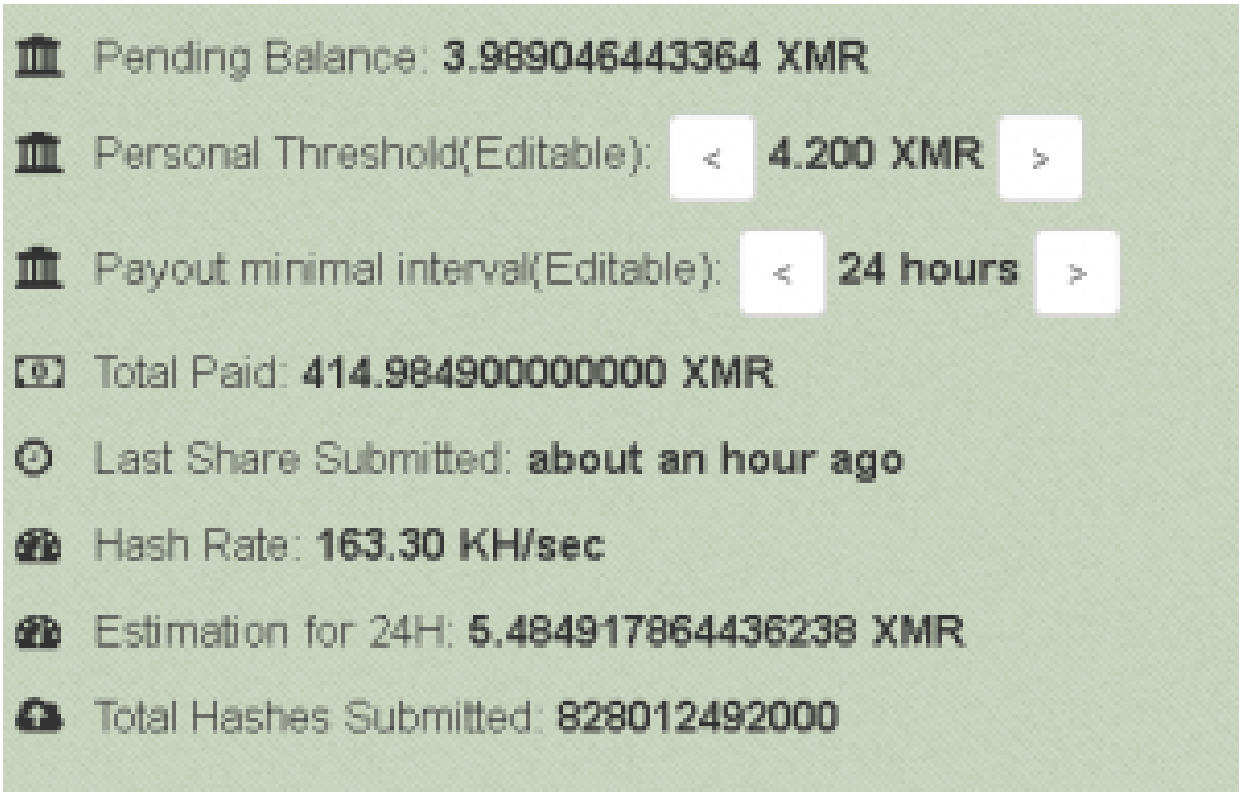

Figure6: Statistics of the attackers' wallet provided by the mining pool

Conclusion

We see that minimal know-how together with very low operating costs and a low risk of getting caught – in this case, misusing legitimate open-source cryptocurrency mining software and targeting old systems likely to be left unpatched – can be sufficient for securing a relatively high outcome.

Sometimes it takes very little to gain a lot, and this is especially true in today's world of cybersecurity, where even well-documented, long-known and warned about vulnerabilities are still very effective due to the lack of awareness of many users.

IoCs

Download Site:
hxxp://postgre.tk
hxxp://ntpserver.tk
Source IPs:
54.197.4.10
52.207.232.106
18.220.190.151
Hashes:
31721AE37835F792EE792D8324E307BA423277AE
A0BC6EA2BFA1D3D895FE8E706737D490D5FE3987
37D4CC67351B2BD8067AB99973C4AFD7090DB1E9
0902181D1B9433B5616763646A089B1BDF428262
0AB00045D0D403F2D8F8865120C1089C09BA4FEE
11D7694987A32A91FB766BA221F9A2DE3C06D173
9FCB3943660203E99C348F17A8801BA077F7CB40
52413AE19BBCDB9339D38A6F305E040FE83DEE1B

If you are interested in this topic you might also be interested in the following:

https://www.welivesecurity.com/2017/09/14/cryptocurrency-web-mining-union-profit/

https://www.welivesecurity.com/2017/09/12/cryptocurrency-state-sponsorship/

Image Credit: © Markéta Fialová

28 Sep 2017 - 02:54PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion