Adylkuzz: Monero Miner Malware

Adylkuzz is a cryptocurrency miner that exploits the vulnerability of Windows software like WannaCry ransomware to generate digital cash. Unlike the WannaCry that locks down a system until a ransom is paid, Adylkuzz allows the computer to work but at the same time generates digital cash or "Monero" cryptocurrency in the background.

More than 200,000 computers have been infected so far and raked in more than $1 million, more than WannaCry ransomware in terms of monetary loss. This cyber attack is still ongoing and may be larger in scale than WannaCry.

Working

The attack is launched from several virtual private servers which are massively scanning the internet on TCP port 445 for potential targets.

Upon successful exploitation via EternalBlue, machines are infected with DoublePulsar. The DoublePulsar backdoor then downloads and runs Adylkuzz from another host. Once running, Adylkuzz will first stop any potential instances of itself already running and block SMB communication to avoid further infection. It then determines the public IP address of the victim and download the mining instructions, cryptominer, and cleanup tools.

It appears that at any given time there are multiple Adylkuzz command and control (C&C) servers hosting the cryptominer binaries and mining instructions.

Symptoms of Infection

Users will experience degradation of computer speeds, bad server performance and lose access to shared Windows resources if their device is infected.

Monero

Monero recently saw a surge in activity after it was adopted by the AlphaBay darknet market, described by law enforcement authorities as “a major underground website known to sell drugs, stolen credit cards and counterfeit items.” Like other cryptocurrencies, Monero increases market capitalization through the process of mining. This process is computationally intensive but rewards miners with funds in the mined currency, currently 7.58 Moneros or roughly $205 at current exchange rates.

There are several Monero addresses associated with this attack as shown in Figures below. By regularly switching addresses, the malware creators are attempting to avoid having too many Moneros paid to a single address.

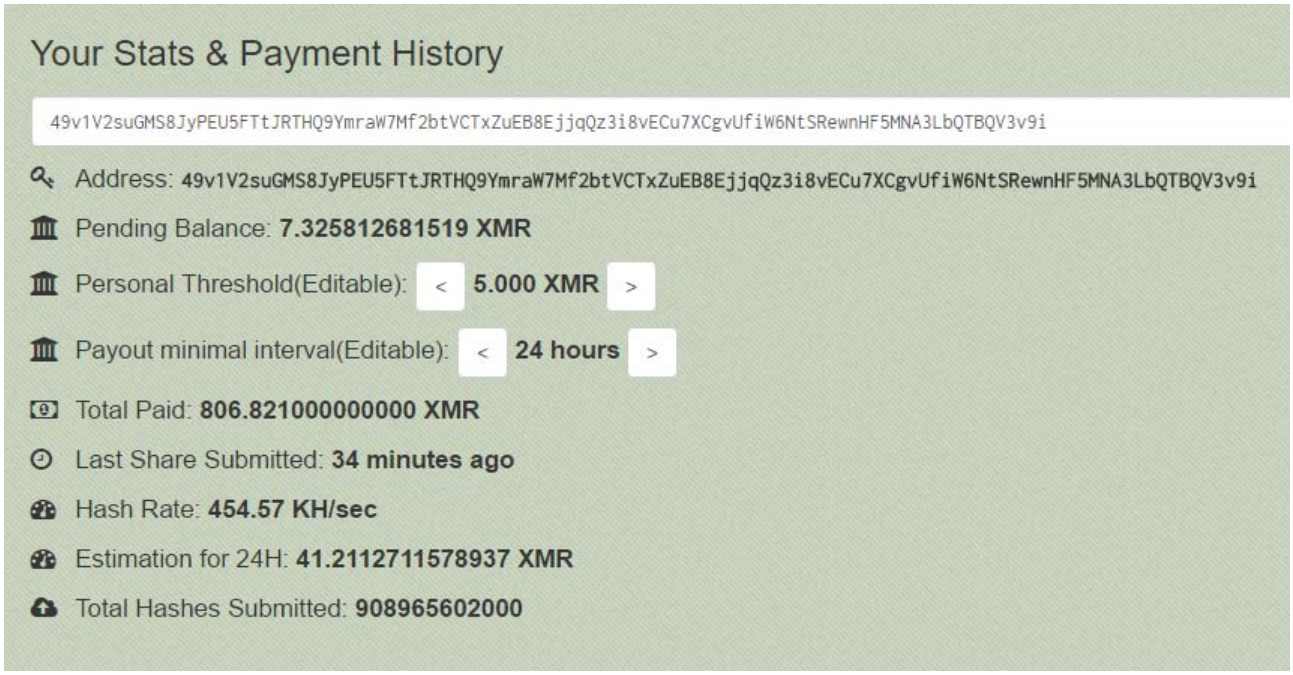

Figure 1

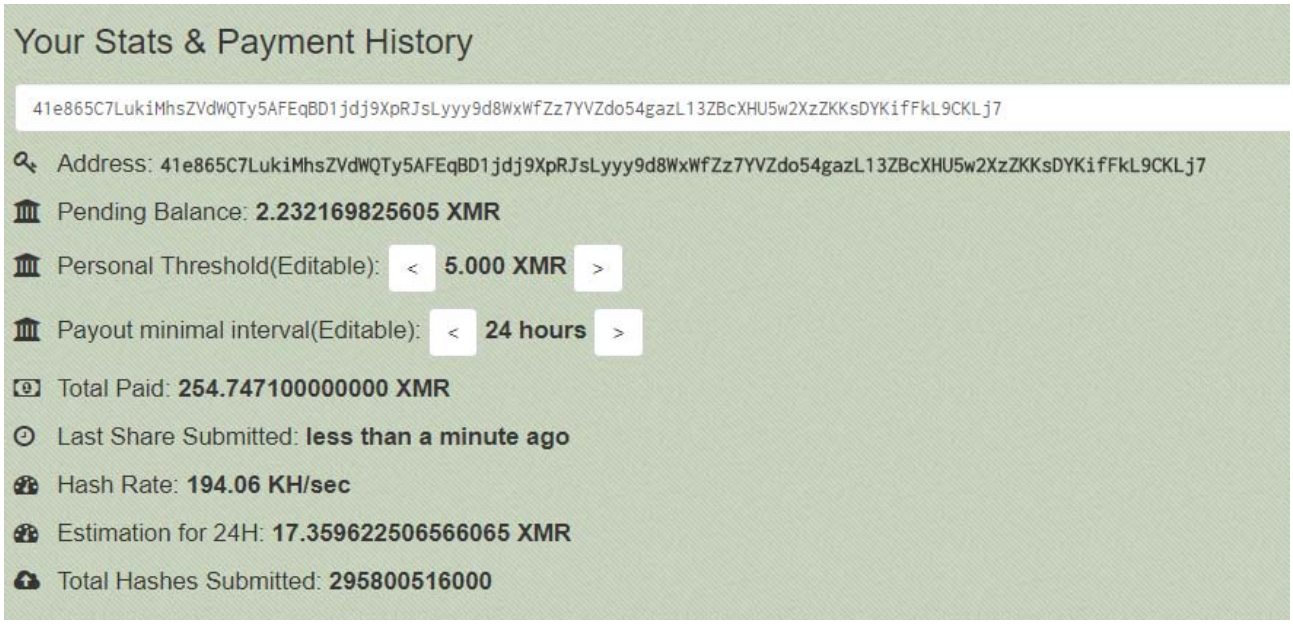

Figure 2

Indicators of Compromise

Selection of Domain/IP Address	Date	Comment
45.32.52[.]8	2017-05-16	Attacking host
45.76.123[.]172	2017-05-16	Attacking host
104.238.185[.]251	2017-05-16	Attacking host
45.77.57[.]194	2017-05-14	Attacking host
45.76.39[.]29	2017-05-15	Attacking host
45.77.57[.]36	2017-05-15	Attacking host
104.238.150[.]145	2017-05-14	Server hosting the payload binary
08.super5566[.]com	2017-05-14	Adylkuzz C&C
a1.super5566[.]com	2017-05-02	Adylkuzz C&C
aa1.super5566[.]com	2017-05-01	Adylkuzz C&C
lll.super1024[.]com	2017-04-24	Adylkuzz C&C
07.super5566[.]com	2017-04-30	Adylkuzz C&C
am.super1024[.]com	2017-04-25	Adylkuzz C&C
05.microsoftcloudserver[.]com	2017-05-12	Adylkuzz C&C
d.disgogoweb[.]com	2017-04-30	Adylkuzz C&C
panel.minecoins18[.]com	2014-10-17	Adylkuzz C&C in 2014
wa.ssr[.]la	2017-04-28	Adylkuzz C&C
45.77.57[.]190	2017-05-15	Host presenting same signature as attackers
45.77.58[.]10	2017-05-15	Host presenting same signature as attackers
45.77.58[.]40	2017-05-15	Host presenting same signature as attackers
45.77.58[.]70	2017-05-15	Host presenting same signature as attackers
45.77.56[.]87	2017-05-15	Host presenting same signature as attackers
45.77.21[.]159	2017-05-15	Attacking Host
45.77.29[.]51	2017-05-15	Host presenting same signature as attackers
45.77.31[.]219	2017-05-15	Host presenting same signature as attackers
45.77.5[.]176	2017-05-15	Host presenting same signature as attackers
45.77.23[.]225	2017-05-15	Host presenting same signature as attackers
45.77.58[.]147	2017-05-15	Host presenting same signature as attackers
45.77.56[.]114	2017-05-15	Host presenting same signature as attackers
45.77.3[.]179	2017-05-15	Host presenting same signature as attackers
45.77.58[.]134	2017-05-15	Host presenting same signature as attackers
45.77.59[.]27	2017-05-15	Host presenting same signature as attackers

Preventive Measures

1. Apply all software patches, especially related to Microsoft Windows OS or Upgrade to latest Windows OS.
2. Back up regularly and keep a recent Encrypted backup copy off-site.
3. Do not open any unsolicited email attachment.

References

1. https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar
2. https://nakedsecurity.sophos.com/2017/05/17/cryptocurrency-mining-malware-cashes-in-on-nsa-exploit-that-enabled-wannacry/
3. https://blog.360totalsecurity.com/en/worse-wannacry-cyberattack-adylkuzz/