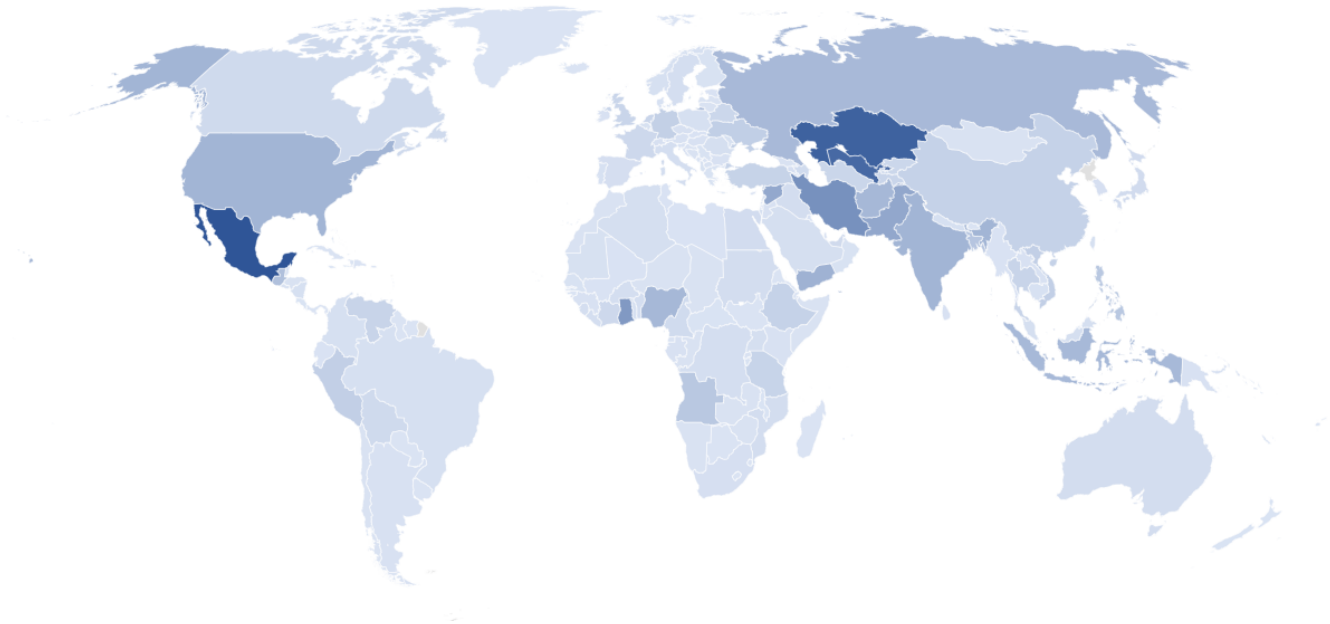
Phorpiex morphs: How a longstanding botnet persists and thrives in the current threat environment

microsoft.com/security/blog/2021/05/20/phorpiex-morphs-how-a-longstanding-botnet-persists-and-thrives-in-the-current-threat-environment/

May 20, 2021



Phorpiex, an enduring botnet known for extortion campaigns and for using old-fashioned worms that spread via removable USB drives and instant messaging apps, began diversifying its infrastructure in recent years to become more resilient and to deliver more dangerous payloads. Today, the Phorphiex botnet continues to maintain a large network of bots and generates wide-ranging malicious activities.

These activities, which traditionally included extortion and spamming activities, have expanded to include cryptocurrency mining. From 2018, we also observed an increase in data exfiltration activities and ransomware delivery, with the bot installer observed to be distributing Avaddon, Knot, BitRansomware (DSoftCrypt/ReadMe), Nemty, GandCrab, and Pony ransomware, among other malware.

The botnet's geographic targeting for bot distribution and installation expanded, too. Previous campaigns focused on targets in Japan, but more recent activity showed a shift to a more global distribution.

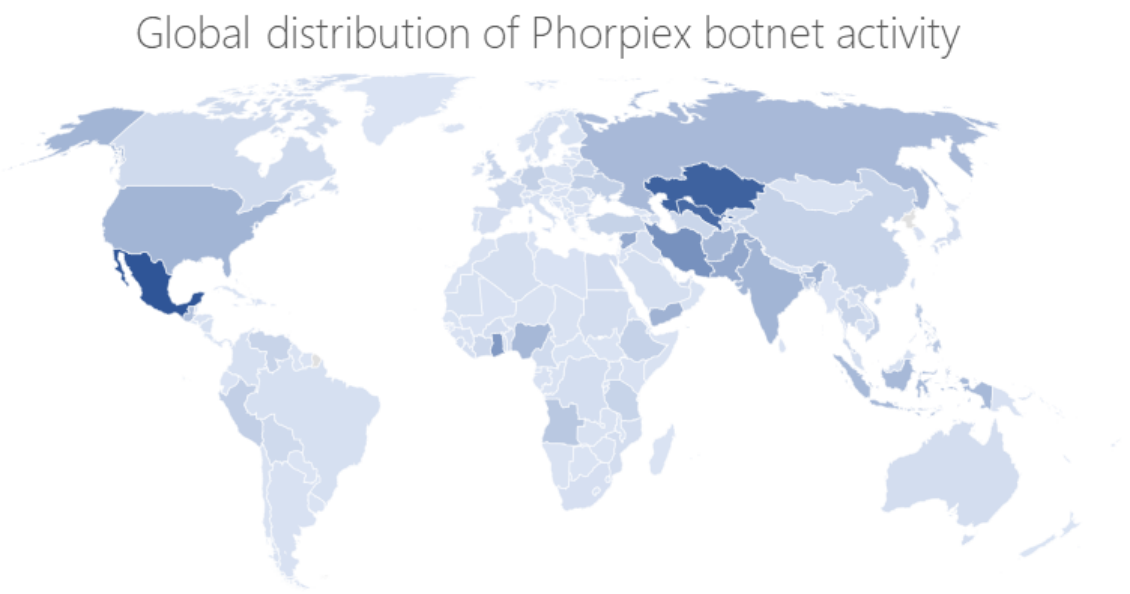


Figure 1. Global distribution of Phorpiex botnet activity

The Phorpiex botnet has a reputation for being simplistic and lacking robustness, and it has been hijacked by security researchers in the past. Its tactics, techniques, and procedures (TTPs) have remained largely static, with common commands, filenames, and execution patterns nearly unchanged from early 2020 to 2021. To support its expansion, however, Phorpiex has shifted some of its previous command-and-control (C2) architecture away from its traditional hosting, favoring domain generation algorithm (DGA) domains over branded and static domains.

This evolution characterizes the role of botnets in the threat landscape and the motivation of attackers to persist and remain effective. The threat ecosystem relies on older botnets with large and diverse network of compromised machines to deliver payloads at low costs. And while many of the older botnet architectures have been primarily classified as spam delivery mechanisms, these infrastructures are critical for newer, modular delivery mechanisms.

Phorpiex also demonstrates that bots, which are some of oldest types of threats, continue to affect consumer users but notably brings increasingly more serious threats to enterprise networks. Despite being traditionally associated with lower-risk activity like extortion and spamming, Phorpiex operators' decision to move to more impactful malware and actions is entirely at the whim of the attackers.

Understanding botnets and associated infrastructure, botnet malware, their activities and payloads, and how they evolve provides insight into attacker motivation and helps ensure durable protection against some of the most prevalent threats today. At Microsoft, we continue to conduct in-depth research into these threats. These expert investigations add to the massive threat intelligence that inform Microsoft 365 Defender services and the protections they provide. Microsoft 365 Defender delivers coordinated cross-domain defense against the various malware, emails, network connections, and malicious activity associated with Phorpiex and other botnets.

Distribution, expansion, and operation

Phorpiex's sprawling botnet operation can be divided into three main portions:

1. Distribution of the bot loader: The bot loader has been propagated through a variety of means over the years, including being loaded by other malware, freeware, and unwanted programs, or delivered by phishing emails from already-infected bots. Phorpiex has also spread via productivity platforms, as well as via instant messaging and USB drives.
2. Mailing botnet: In addition to spreading the bot loader via email, the botnet is used to generate currency. It does so via extortion and spam campaigns as well as through a variety of other types of financially motivated malware.
3. Malware delivery botnet: In recent years, the botnet has been observed installing ransomware, cryptocurrency miner, and other malware types, indicating the expansion of the botnet's activities by the Phorpiex operators or as part of malware-as-a-service scheme.

From December 2020 to February 2021, the Phorpiex bot loader was encountered in 160 countries, with Mexico, Kazakhstan, and Uzbekistan registering the most encounters.

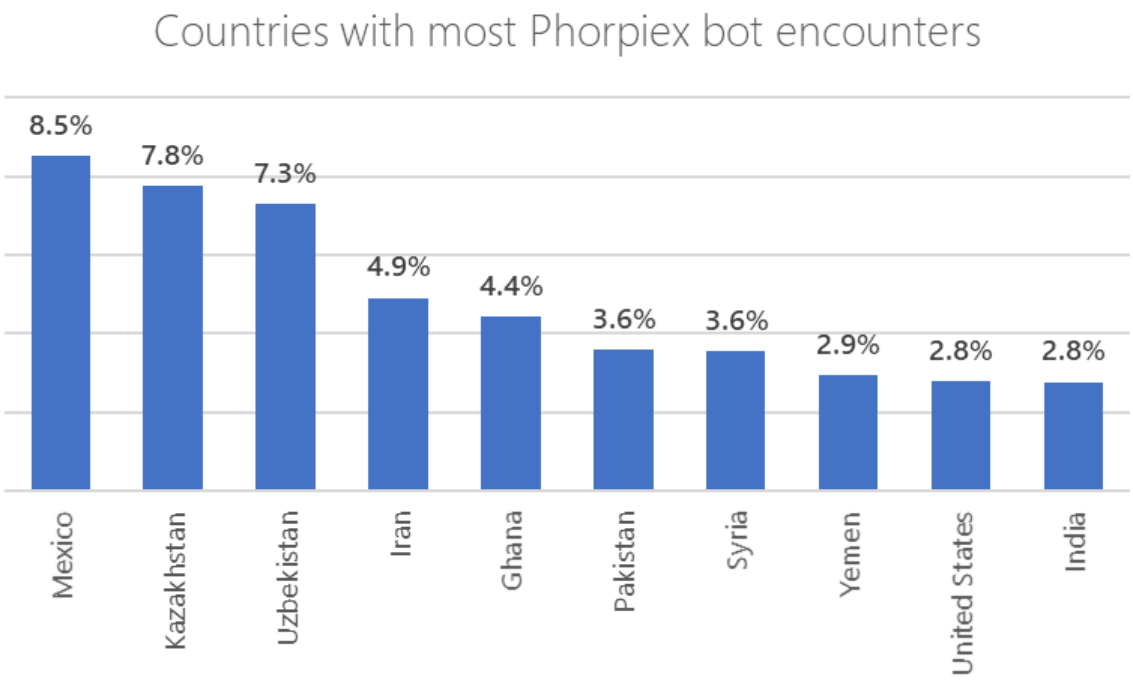


Figure 2. Countries with the most encounters of the Phorpiex bot loader

In December 2020 and January 2021, we observed non-weaponized staging of Knot ransomware on Phorpiex servers. In February, we also detected commodity malware such as Mondfoxia (also known as DiamondFox) in these servers. These recent developments indicate new loader and monetization strategies under active development.

The combination of the wide variety of infection vectors and outcomes makes the Phorpiex botnet appear chaotic at first glance. However, for many years Phorpiex has maintained a consistent internal infrastructure using similar domains, command-and-control (C2) mechanisms, and source code.

The wide range of infection vectors used by Phorpiex requires a unified security approach that ensures protection is delivered on the endpoint, network, email, and applications. Microsoft 365 Defender's advanced threat protection technologies detect malicious activity in each of these domains. Moreover, the correlation of these cross-domain threat data surfaces additional malicious activity, allowing Microsoft 365 Defender to provide coordinated and comprehensive protection against Phorpiex.

Bot distribution and installation

Phorpiex maintains and expands its network of bot-infected computers by distributing the Phorpiex bot loader. In 2020 and 2021 we observed the bot loader being spread through Phorpiex bot-delivered emails with .zip or other archive file attachments, downloaded from fake download sites for software (such as photo editing software, screensaver, or media players), or downloaded by other malware also delivered through email. These multiple entry points demonstrate the modular nature of the malware economy.

Regardless of distribution mechanism, however, the bot loader operates in a fairly uniform fashion. It uses three distinct types of C2 to fulfil different goals during and after installation:

- Downloading the Phorpiex malware implant
- Downloading updates to the Phorpiex implant and new exploit modules
- Checking in with C2 infrastructure to deliver cryptocurrency or return data

The malware implant is initially downloaded from sites such as *trik[.]ws* (historically) or, more recently, a malware hosting repository, *worm[.]ws*. We are also noticing a shift to using more dedicated IP-based C2 and delivery sites, such as *185[.]215[.]113[.]10* and *185[.]215[.]113[.]8*. A notable Phorpiex behavior is the downloading of numbered modules, typically numbered 1-10, with URL paths such as <domain>.com/1, <domain>.com/2, <domain>.com/3, continuing this pattern for as

many additional components as needed. As these downloads do not happen through standard web traffic, network-level protection is necessary to prevent malicious downloads. In a very recent development, we observed that most Phorpiex bot loader malware have abandoned branded C2 domains and have completely moved to using IPs or DGA domains. However, as in the past, the operators neglected to register all the potential sites that the DGA domains resolve to.

When downloaded and run, the implant attempts to connect to legitimate external sites like *WIPMANIA.com* to get IP information. It does this repeatedly during subsequent check-ins, and then begins connecting to hardcoded C2 servers. During these check-ins, the implant checks the device's regional settings and exits if it's operating in a non-desired region, such as Ukraine. Favored regions include countries in East Asia as well as English-speaking countries.

The loader modules and updates are pulled from a variety of attacker-owned domains. These domain-names typically begin with a second-level domain (2LD) of TLDR, TSRV, or THAUS and end with an assortment of unorthodox TLD such as .WS, .TOP, .RU, .CO, .TO, .SU., .CC, and .IO. As has been pointed out by other researchers, the TSRV and TLDR are likely references to "Trik Server" or "Trik Loader", as many of the internals of the malware use Trik as proprietary name.

Regular connections to these attacker-owned domains continue during infection, such that devices that have been infected for months receive new loader versions and capabilities. Modules downloaded from C2 can include additional malware, ransomware, cryptocurrency mining functionality, worming functionality, and the Phorpiex mailing botnet functionality. It is most common for a bot to be participating in mailing and crypto mining, as these seem to be driving revenue generation for the operators during non-ransomware initiatives.

The bot also establishes persistence and attempts to disable security controls. This includes modifying registry keys to disable firewall and antivirus popups or functionality, overriding proxy and browser settings, setting the loader and executables to run at startup, and adding these executables to the authorized application lists. A sample of the keys changed is below, with minor changes from version to version of the loader:

- *\FirewallPolicy\StandardProfile\AuthorizedApplications\List*
- *\Microsoft\Windows\CurrentVersion\Run\Host Process for Windows Services*
- *\Microsoft\Security Center\AntiVirusOverride*
- *\Microsoft\Security Center\AntiVirusDisableNotify*
- *\Microsoft\Security Center\FirewallOverride*
- *\Microsoft\Security Center\FirewallDisableNotify*
- *\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings*
- *\Microsoft\Security Center\UpdatesOverride*
- *\Microsoft\Security Center\UpdatesDisableNotify*
- *\Microsoft\Windows NT\CurrentVersion\SystemRestore*
- *\Microsoft\Windows Defender\Real-Time Protection\DisableBehaviorMonitoring*
- *\Microsoft\Windows Defender\Real-Time Protection\DisableOnAccessProtection*
- *\Microsoft\Windows Defender\Real-Time Protection\DisableScanOnRealtimeEnable*

Enabling tamper protection in Microsoft Defender for Endpoint prevents the bot from making modifications related to Microsoft Defender services. Microsoft Defender for Endpoint automatically cleans up changes made by the bot (if any) during threat cleanup and remediation. Security operations teams can use advanced hunting capabilities to locate these and similar modifications. Administrators can also disable "Local Policy Merge" to prevent local firewall policies from getting in effect over group policies.

As the bot loader updates, the key values change to reflect new files, randomized file paths, and masqueraded system files. The example below illustrates a change from SVCHOST to LSASS:

KEY NAME: HKEY_CURRENT_USER\[ID]\Software\Microsoft\Windows\CurrentVersion\Run
OLD VALUE: C:\1446621146296\svchost.exe
NEW VALUE: C:\19197205241657\lsass.exe

At varying intervals, the bot implant collects lists of files and exfiltrates that data to external IP addresses leased by the attacker, many of which also serve as C2. When additional malware is installed, the pull is initiated from the implant itself. The malware is staged on the Phorpiex operators' servers prior to new campaigns or on the shared sites such *as worm[.]ws*.

The bot checks in routinely, often weekly and sometimes even daily. It does this to upload any outcomes from the various modules that the bot installs, such as coin mining deposits or spam activity.

In addition to detecting and blocking the bot malware through its endpoint protection platform (EPP) and endpoint detection and response (EDR) capabilities, Microsoft Defender for Endpoint's network protection defends against botnet activities like connecting to attacker-controlled servers, mimicking system files, and downloading implants and additional payloads.

Self-spreading via remote drives

One of the more unique and easily identifiable Phorpiex behavior when it spread primarily via USB involves a check that occurs routinely for all connected remote drives. The bot then creates a series of hidden folders on those drives with underscores (e.g., "__") and then changes the registry attributes to make these appear invisible to the user. The bot then copies all its file configurations and include a malicious *DriveMgr.exeI*, a copy of the loader, as well as a .lnk file that runs the malware when opened. This activity has been largely consistent since 2019. This functionality offers a self-spreading mechanism that offers a backup way to expand the bot implant base. Commands consistent with this Phorpiex worming activity are:

- *ShEllExECutE=__\\DriveMgr.exe*
- *"cmd.exe" /c start __ & __\DriveMgr.exe & exit*

Microsoft Defender for Endpoint offers multiple layers of protection against USB threats. This includes real-time scanning of removable drives and attack surface reduction rule to block untrusted and unsigned processes that run from USB. Microsoft Defender for Endpoint also enables organizations to monitor and control removable drives, for example allow or block USB based on granular configurations, and monitor USB activities.

Phorpiex as a mailing botnet

For several years, Phorpiex used infected machines to deliver extortion, malware, phishing, and other content through large-scale email campaigns. These emails span a large set of lures, subject lines, languages, and recipients, but there are key sets of characteristics that can identify emails sent from the Phorpiex botnet:

- Spoofed sender domain, sender username, and sender display name
- Sender domain of 4 random digits
- Sender username using a generic name with a variety of numbers
- Subjects or lures referencing singular names, heights and weights, surveillance
- Body of the message often referencing dating services or extortion material for ransom
- Presence of Bitcoin, DASH, Etherium, or other cryptocurrency wallets
- ZIP files or other file types purporting to be images such as JPG files or photo types

These patterns include language more commonly used in consumer extortion emails, which reference having illicit photos or videos of the recipient. These are also the same lures that are used to distribute the bot installer as well as ransomware or other malware. The messages often include old passwords of individuals gathered from publicly available lists, a method that attackers use to add credibility whether the mail is received in a corporate environment or at home.

Microsoft Defender for Office 365 detects malicious emails sent by the Phorpiex botnet. These include the extortion and phishing emails, as well as messages carrying malware, whether the Phorpiex loader itself or other malware. Microsoft Defender for Office 365 users AI and machine learning to detect user and domain impersonation, informed by its comprehensive visibility into email threats as well as through in-depth research like this.

Spam and extortion campaigns

Phorpiex is well known for illicit image or video-based extortion phish and spam campaigns, also known as "sextortion". These campaigns target a large variety of regions and languages, which is a different set of targets from bot distribution activities. These generally do not deliver malware directly. They are meant to collect revenue for the operator by asserting that they have already compromised a device and have access to damaging material regarding the recipient.

Sextortion campaigns have been quite popular in recent years and generally require payment from the victim in cryptocurrency. We observed Phorpiex operators requiring payment primarily through Bitcoin and Dash. Examples of one such cryptocurrency profit volume from a campaign in late February 2021 targeting English speaking users is below, with the subject "Payment from your account".

There are several public monitors of extortion wallets operated by Phorpiex, which have seen the operators of the botnet running numerous wallets during any given week. We observed the below example in which an operator requested $950 from users and accumulated over $13,000 in 10 days.

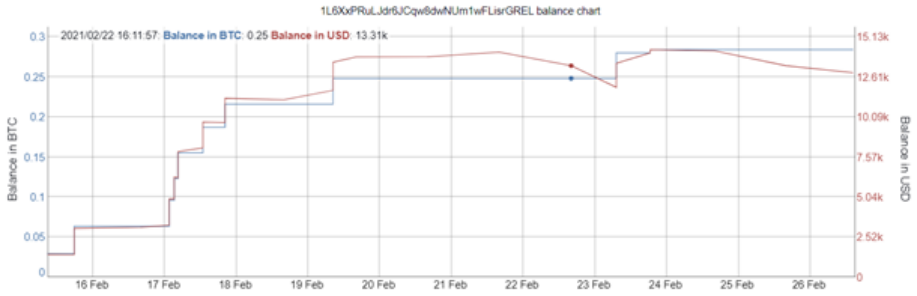


Figure 3. Cryptocurrency profit volume from a single wallet used in spam extortion campaign in late February 2021. Data from BitInfoCharts.

In late 2020 and early 2021 we also observed this extortion scheme exploiting fears about security vulnerabilities in teleconferencing applications such as Zoom. The messages claimed that a vulnerability is what allowed the operators to capture their extortion material.

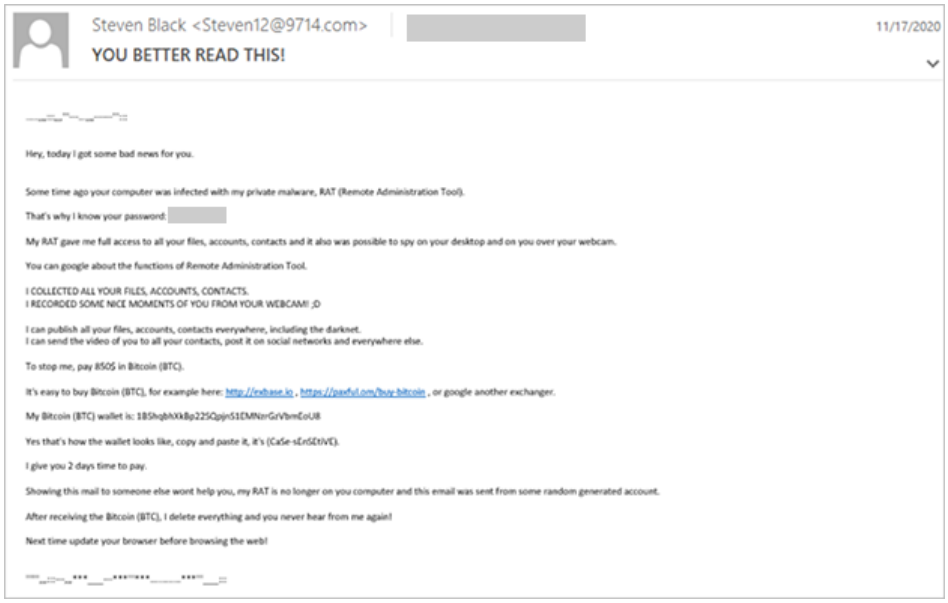


Figure 4. Example of an extortion email lure from late 2020

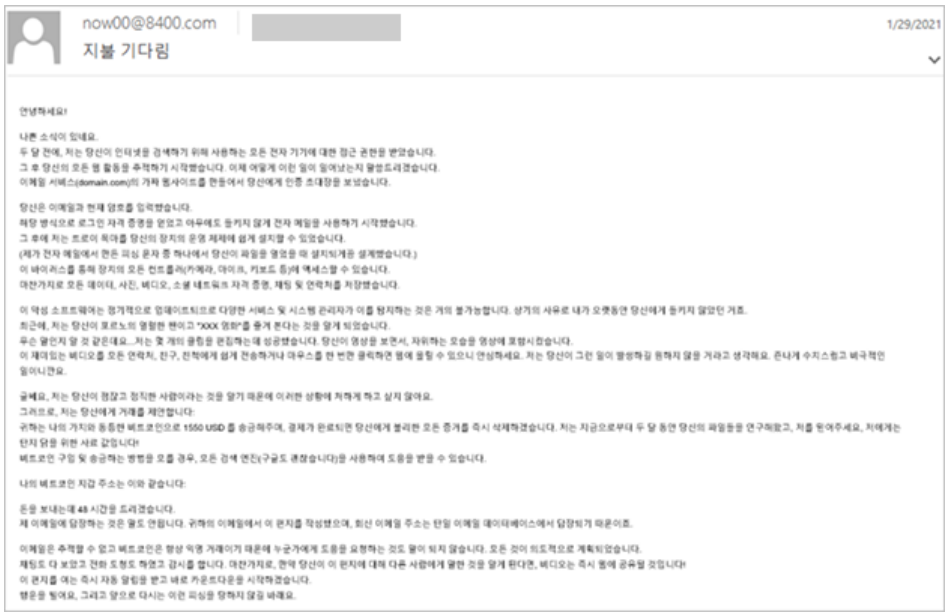


Figure 5. Example of a Korean language extortion email lure from early 2021

In addition to the examples above, Phorpiex is often distributed via business email compromise and contain no links or URLs. This hampers many automatic detection capabilities an organization might have in place.

Phishing, malware, and ransomware campaigns

Phorpiex-powered phishing campaigns as well as bot implant installations deliver secondary malware as well as standard extortion and spam. The tactics involving the spread of emails are the same, with the only differences being in the attachments or links. Malware involving malicious Office documents is interspersed with deliveries of the bot implant or direct ransomware deliveries, which are often contained within .ZIP attachments.

Since 2019, many of the malware-carrying emails from Phorpiex use the same lures, subject lines, and attachment file names. The emails use a randomly generated feminine name in the subject or reference an embarrassing or improperly obtained photo, and either contain extortion or deliver ransomware. As part of the social engineering lure, he malware attachments masquerade as .jpg files or other file types, while appearing as .zip or .js files.

Figure 6. Example of an email lure including malicious ZIP attachment masquerading as an image of an actress

In Summer and Fall 2020 many new Phorpiex infections began to spread using archive files to deliver BitRansomware and Avaddon. Avaddon only began spreading in mid to late 2020 and its distribution seems to have been tightly coupled with Phorpiex since its inception.

In the month of August 2020, there was also an increase in the number of bot implants installed on devices, corresponding with the ransomware increase. At this time, most instances of ransomware perpetrated by Phorpiex were carried through the bot implant itself.

Phorpiex as malware delivery botnet

In addition to operating as a mailing botnet, Phorpiex has evolved to deliver other malware as well, most notably cryptocurrency mining malware and ransomware.

Cryptocurrency mining malware

In 2019 Phorpiex started utilizing an XMRIG miner to monetize the hosts with Monero. This module is included in almost all bot installations at the time of infection and communicates primarily over port 5555. This behavior might be coupled with other malware, but in this instance, it is associated with the masqueraded system process used by the rest of the Phorpiex implant (i.e., *SVCHOST.exe* or *LSASS.exe*).

The miner is downloaded as a module masquerading as *WINSYSDRV.exe* It stores its configuration locally and checks it periodically. The miner does this from additional masqueraded system processes injected into legitimate processes to read its configuration and to mine.

The *WINSYSDRV.exe* file routinely kicks off a series of heavily nested processes preceded by a PING with a long wait, which is intended to avoid sandboxes. This command is shown below:

cmd.exe /C ping [INTERNAL IP] -n 8 -w 3000 > Nul & Del /f /q "C:\ProgramData\PnQssBdbSh\winsysdrv.exe" & "C:\Users\[USER]\AppData\Local\Temp\winsysdrv.exe"

In prior versions, this command utilized the legitimate but hijacked *WUAPP.exe* process. Recently we have seen *NOTEPAD.exe* used to read the path, which is a variant of *C:\ProgramData\[RandomString]cfg*:

- "C:\Windows\System32\wuapp.exe" -c "C:\ProgramData\ADwXcSSGvY\cfgi" (2019-2020)
- "C:\Windows\System32\wuapp.exe" -c "C:\ProgramData\PnQssBdbSh\cfgi" (2020)
- "notepad.exe" -c "C:\ProgramData\PnQssBdbSh\cfgi" (2020-2021)
- "notepad.exe" -c "C:\ProgramData\PnQssBdbSh\cfg" (2020-2021)

In addition to mining Monero, versions of the bot loader also upload to Bitcoin wallets. We were able to scrape those addresses via downstream executables dropped by the Phorpiex loader masquerading as *SVCHOST.exe* or *LSASS.exe*. Below is an example of the balance in one such wallet address that was active from September to November 2020, embedded in a specific sample.

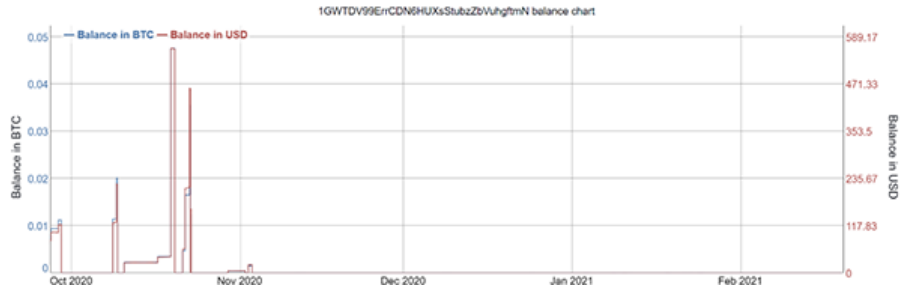


Figure 7. Cryptocurrency profit from a single wallet used in a miner dropped on an infected machine from September to November 2020. Data from BitInfoCharts.

In February of 2021, infected implants also downloaded additional Etherium miners. These miners create scheduled tasks are labeled "WindowsUpdate" but run the miner every minute. The miners search for graphics cards as well as other resources to use for mining with an *ethermine.org* mining pool. Here's an example task creation:

schtasks /create /sc minute /mo 1 /tn WindowsUpdate /tr %TEMP%\System.exe

Microsoft has also observed Phorpiex variants with cryptocurrency-clipping functionality accompanying the installation of the loader. In these instances, the malware checks clipboard values for a valid cryptocurrency wallet ID. If it finds one, it sets its own hardcoded value. This method allows attackers to profit from existing mining installations or prior malware without having to bring in new software or remove old instances.

Microsoft Defender for Endpoint detects and blocks cryptocurrency mining malware and coin mining activity in general. To continue enhancing this detection capability, Microsoft recently integrated Intel Threat Detection Technology (TDT) into Microsoft Defender for Endpoint, allowing our endpoint detection and response capabilities to use silicon-based threat detection to better protect against coin mining malware.

Ransomware

Phorpiex has been associated with multiple ransomware families through the years. Phorpiex either delivers ransomware on behalf of other groups using those operators' infrastructure or host the ransomware themselves. The latter is more common in the case of commodity kits like Avaddon and Knot.

As recently as February 2021, Avaddon was under active development. Like the Phorpiex loader itself, Avaddon performs language and regional checks for Russia or Ukraine before running to ensure only favored regions are targeted.

The initial Avaddon executable is located in the TEMP folder, and it generally uses a series of random characters as file extension for encrypted files. Before deleting backups and encrypting the drive, it validates that UAC is disabled by checking if certain registry keys are set to "0", modifying the value if not:

- \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA = "0"
- \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin = "0"
- \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLinkedConnections = "1"

After achieving the privilege level needed, encryption usually occurs on the individual machine without lateral movement, though that is subject to change based on the operator's monetization strategy. The procedure for deleting backups, like most ransomware, is performed with the following commands:

- *cmd /c wmic.exe SHADOWCOPY /nointeractive*
- *cmd /c wbadmin DELETE SYSTEMSTATEBACKUP*
- *cmd /c wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest*
- *cmd /c bcdedit.exe /set {default} recoveryenabled No*
- *cmd /c bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures*
- *cmd /c vssadmin.exe Delete Shadows /All /Quiet*

Microsoft Defender for Endpoint detects and blocks the ransomware. It also detects and raises the following alerts for the encryption and backup deletion behaviors, enabling security operations teams to be notified and immediately respond to ransomware activity on their environment:

- Ransomware behavior detected in the file system
- File backups were deleted

We have observed that the external commands and behaviors of the Avaddon ransomware have largely remained the same since its introduction in June-July 2020. This includes the tendency to masquerade as the system file *Taskhost.exe*. Avaddon, which demands a ransom in Bitcoin equivalent to $700, is still active today and being actively distributed by Phorpiex using new bot loaders that are not substantially different in behavior. Microsoft Defender for Endpoint continues to provide durable protection against these new campaigns.

Other ransomware is slightly less common lately, but in December 2020, a non-weaponized version of Knot ransomware was staged on Phorpiex-operated servers. It did not seem to have had any infections yet as this may have been a test version. This ransomware shares a high degree of similarity to the Phorpiex loader itself and improved versions have not yet been seen. Like Avaddon, Knot typically demands relatively smaller sums of money in Bitcoin, equivalent to $350. The ransom notes generally require Bitcoin payment to a wallet, though no payments seem to have been made that month.

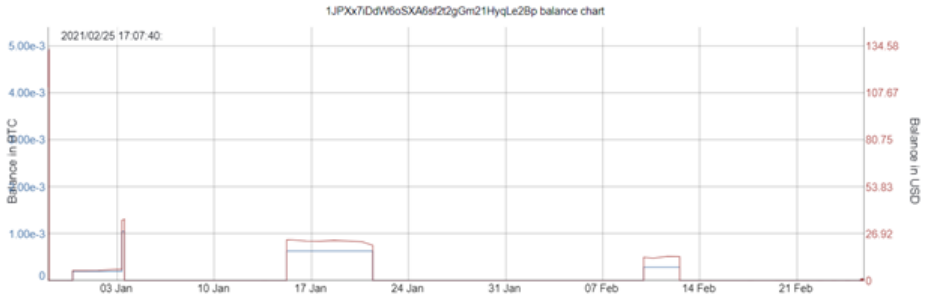


Figure 8. Cryptocurrency profit volume from a single wallet attached to a Knot ransomware sample in early 2021, showing no payments of the asking price. Data from BitInfoCharts.

Defending against botnets and associated activity

Botnets drive a huge portion of the malware economy, and as the resilience of Phorpiex shows, they evolve to adapt to the ever-changing threat environment. Our many years of experience analyzing, monitoring, and even working with law enforcement and other partners to take down botnets tell us that alternative infrastructures rise as attackers try to fill in the void left by disrupted botnets. Typically, new infrastructures are born as a result of these movements, but in the case of Phorpiex, an established botnet adapts and takes over.

The wide range of malicious activities associated with botnets, as we detailed in this in-depth research into Phorpiex, represent the spectrum of threats that organizations face today: various attack vectors, multiple spreading mechanisms, and a diverse set of payloads that attackers can change at will. To combat these threats, organizations need security solutions that deliver cross-domain visibility and coordinated defense.

Microsoft 365 Defender leverages the capabilities and signals from the Microsoft 365 security portfolio to correlate threat data from endpoints, email and data, identities, and cloud apps to provide comprehensive protection against threats. Microsoft Defender for Endpoint detects and blocks malware, other malicious artifacts, and malicious behavior associated with botnet activity, as well as the deployment of secondary payloads like cryptocurrency miners and ransomware. Features like attack surface reduction, tamper protection, and security controls for removable media further help prevent these attacks and harden networks against threats in general. Microsoft Defender for Office 365 detects the malicious attachments and URLs in emails generated by the mailing operations of the Phorpiex botnet.

Our industry-leading visibility informs AI and machine learning technologies that power the automatic prevention, detection, and remediation of threats, as well as the rich set of investigation tools available to defenders for hunting, analyzing, and resolving attacks. The recently generally available unified Microsoft 365 Defender security center integrates capabilities so defenders can manage all endpoint, email, and cross-product investigations, configuration, and remediation with a single portal.

Our understanding of how botnets operate and evolve, through in-depth research like this, further enriches our ability to continue delivering defenses against the threats of today and the future. Learn how Microsoft 365 Defender stops attacks with automated, cross-domain security and built-in AI.

Microsoft 365 Defender Threat Intelligence Team

Advanced hunting

The Phorpiex botnet used highly varied payloads and delivery methods after email distribution. You can use the provided advanced hunting queries to surface activities associated with Phorpiex and similar threats.

Phorpiex variable command-and-control connections

Looks for a series of registered and unregistered delivery and installation domains that have been used by Phorpiex upon installation of the bot implant and at regular intervals for updates of the bot implant. These network connections are often initiated by the DriveMgr process or one of the later faked system processes. Regex was included to limit scope and for use in other queries based on all of the currently known URL paths associated with Phorpiex component downloads such as cc11, cc22 and, others. Regex and RemoteUrl statements can be removed if query is slow in a particular environment or to gather more results from broad DriveMgr.exe network connections. Run query.

```
DeviceNetworkEvents
| where InitiatingProcessFileName == "DriveMgr.exe"
| where RemoteUrl has ("api.wipmania.com") or
RemoteUrl matches regex "\\/(([a-z]{2}[0-6]{2})|([0-6]{2}[a-z]{2})|([0-6]{1,2})|
(pepwn|t|m|r|s|p|consensus.z))(\\.exe)?"
```

Phorpiex bot Implant DriveMgr strings

Looks for a series of persistent strings used in the Phorpiex bot implant for self-replication via removable drives. This implant will often search for any removable drives and create hidden empty folders to copy the loader to. This offers Phorpiex a way of self-propagation via the removable drives or attached storage and appears invisible to the user of the drive. This has occasionally been reused in other named worms but is most common in Phorpiex, especially if accompanied by C2 activity. Run query.

```
DeviceProcessEvents
| where InitiatingProcessFileName == "cmd.exe"
| where InitiatingProcessCommandLine has "\\DriveMgr.exe & exit"
```

Phorpiex masqueraded system process network activity

Looks for a pattern of a system process executable name that is not legitimate and running from a folder that is created via a random algorithm 13-15 numbers long. This pattern has changed slightly over time, but this is the current iteration as of May 2021. The portions that are most likely to change are the service names and the length of the random pattern and the explicit faked process name. Run query.

```
let FakeProcesses =
pack_array("lsass.exe","svchost.exe","audiodg.exe","wininet.exe","winmanager.exe","smss.exe","sedsvc.exe",
"csrss.exe","winmanager.exe","dllhost.exe","drivemgr.exe","winsysdrv.exe","winsvcs.exe","notepad.exe");
DeviceNetworkEvents
| where InitiatingProcessFileName in (FakeProcesses)
| where InitiatingProcessFolderPath matches regex "\\\\[\\d]{13,15}"
```

Indicators

Non-DGA domains

tsrv1[.]com	tsrv1[.]ws	tsrv2[.]top
tsrv3[.]ru	tsrv4[.]ws	tsrv5[.]top
tldrbox[.]com	tldrbox[.]top	tldrbox[.]ws
tldrhaus[.]top	tldrnet[.]top	tldrzone[.]com
tldrzone[.]top	tsrv2[.]ws	tsrv3[.]ws
thaus[.]ws	worm[.]ws	thaus[.]to
gotsomefile[.]top	feedmefile[.]top	gotsomefile[.]top
xmrupdtemall[.]top	vitamind[.]top	w4tw4tw4tw4t4[.]jo

DGA domain samples

aiiaiafrzrueuedur[.]ru	afeifieuuufufufuf[.]su	ssofhoseuegsgrfnj[.]su
uoaeogauhduadhug[.]su	aeiziaezieidiebg[.]su	osheoufhusheoghuesd[.]ru
plpanaifheaighai[.]su	rzhsudhugugfugugsh[.]co	ndrxbezrsdgsergdfs[.]co
bfagzzezgaegzgfaih[.]co	aegohaohuoruitiieh[.]co	gaoehuoaoefhuhfugh[.]co
gaghpaheiafhjefijh[.]co	gaohrhurhuhruhfsdh[.]co	eaeuafhuaegfugeudh[.]co
befaheaiudeuhughgh[.]co	aefofhhfouahugr[.]ws	urusurofhsorhfuuhd[.]io
afaeigaifgsgrhhafd[.]io	eaougheofhuaez[.]top	seuufhehfueughem[.]top
seuufhehfueughek[.]ws	feauhueudughuurk[.]ws	eafueudzefverrgk[.]ws
eafuebdbedbedggk[.]ws	efeuafubeubaefur[.]ws	eafuebdbedbedggr[.]ws
gaueudbuwdbuguur[.]ws	okdoekeoehghaoer[.]ws	eafueudzefverrgr[.]ws
geaohgoehagugeh[.]su	zrziqezrizrizzf[.]su	efaejfojegohgut[.]su
zzruuoooshfrohu[.]su	osheoufhusheoghuesd[.]ru	ouhfuosuoosrhfzr[.]su
rubbfibididhiei[.]ru	koekfoaejfoefok[.]ru	aeguaheoufuhfhu[.]ru

gaehaejehgaefgz[.]ru	ploeuahfueugeug[.]ru	efniaenfinefing[.]ru
mokaeduegfuaehh[.]ru	geafneiefiefnin[.]ru	loeofaihefihfhg[.]ru
awwararuhuedhhf[.]ru	aefiaefidjidghh[.]ru	lpiauefhuheufhg[.]ru
aeaagegaegeahrh[.]ru	mnenneaihfihegi[.]ru	avdbawudhafiehf[.]ru
efaejfojegohgut[.]ru	geaohgoehagugeh[.]ru	zrziqezrizrizzf[.]ru
aoekfoaefoahfoh[.]ru	ebufaehfahefheh[.]ru	rohgoruhgsorhugih[.]ru
unokaoeojoejfghr[.]ru	aeifaeifhutuhuhusr[.]su	urusurofhsorhfuuhr[.]su
rzhsudhugugfugugsr[.]su	bfagzzezgaegzgfair[.]su	eaeuafhuaegfugeudr[.]su
aeufuaehfiuehfuhfr[.]su	daedagheauehfuuhfr[.]su	aeoughaoheguaoehdr[.]su
eguaheoghouughahsr[.]su	huaeokaefoaeguaehr[.]su	afaeigaifgsgrhhafr[.]su
afaigaeigieufuifir[.]su	geauhouefheuutiiir[.]su	gaoheeuofhefefhutr[.]su
gaouehaehfoaeajrsr[.]su	gaohrhurhuhruhfsdr[.]su	gaghpaheiafhjefijr[.]su
gaoehuoaoefhuhfugr[.]su	aegohaohuoruitiier[.]su	befaheaiudeuhughgr[.]su
urusurofhsorhfuuhz[.]io	aeifaeifhutuhuhusz[.]io	rzhsudhugugfugugsz[.]io
bfagzzezgaegzgfaiz[.]io	eaeuafhuaegfugeudz[.]io	aeufuaehfiuehfuhfz[.]io
daedagheauehfuuhfz[.]io	aeoughaoheguaoehdz[.]io	eguaheoghouughahsz[.]io
huaeokaefoaeguaehz[.]io	afaeigaifgsgrhhafz[.]io	afaigaeigieufuifiz[.]io
geauhouefheuutiiiz[.]io	gaoheeuofhefefhutz[.]io	gaouehaehfoaeajrsz[.]io
gaohrhurhuhruhfsdz[.]io	gaghpaheiafhjefijz[.]io	gaoehuoaoefhuhfugz[.]io
aegohaohuoruitiiez[.]io	befaheaiudeuhughgz[.]io	urusurofhsorhfuuhu[.]cc
aeifaeifhutuhuhusu[.]cc	rzhsudhugugfugugsu[.]cc	bfagzzezgaegzgfaiu[.]cc
eaeuafhuaegfugeudu[.]cc	aeufuaehfiuehfuhfu[.]cc	daedagheauehfuuhfu[.]cc
aeoughaoheguaoehdu[.]cc	eguaheoghouughahsu[.]cc	huaeokaefoaeguaehu[.]cc
afaeigaifgsgrhhafu[.]cc	afaigaeigieufuifiu[.]cc	geauhouefheuutiiiu[.]cc
gaoheeuofhefefhutu[.]cc	gaouehaehfoaeajrsu[.]cc	gaohrhurhuhruhfsdu[.]cc
gaghpaheiafhjefiju[.]cc	gaoehuoaoefhuhfugu[.]cc	aegohaohuoruitiieu[.]cc
befaheaiudeuhughgu[.]cc	urusurofhsorhfuuhl[.]co	aeifaeifhutuhuhusl[.]co
rzhsudhugugfugugsl[.]co	bfagzzezgaegzgfail[.]co	eaeuafhuaegfugeudl[.]co
aeufuaehfiuehfuhfl[.]co	daedagheauehfuuhfl[.]co	aeoughaoheguaoehdl[.]co
eguaheoghouughahsl[.]co	huaeokaefoaeguaehl[.]co	afaeigaifgsgrhhafl[.]co
afaigaeigieufuifil[.]co	geauhouefheuutiiil[.]co	gaoheeuofhefefhutl[.]co
gaouehaehfoaeajrsl[.]co	gaohrhurhuhruhfsdl[.]co	gaghpaheiafhjefijl[.]co
gaoehuoaoefhuhfugl[.]co	aegohaohuoruitiiel[.]co	befaheaiudeuhughgl[.]co
urusurofhsorhfuuhm[.]to	aeifaeifhutuhuhusm[.]to	rzhsudhugugfugugsm[.]to
bfagzzezgaegzgfaim[.]to	eaeuafhuaegfugeudm[.]to	aeufuaehfiuehfuhfm[.]to

daedagheauehfuuhfm[.]to	aeoughaoheguaoehdm[.]to	eguaheoghouughahsm[.]to
huaeokaefoaeguaehm[.]to	afaeigaifgsgrhhafm[.]to	afaigaeigieufuifim[.]to
geauhouefheuutiiim[.]to	gaoheeuofhefefhutm[.]to	gaouehaehfoaeajrsm[.]to
gaohrhurhuhruhfsdm[.]to	gaghpaheiafhjefijm[.]to	gaoehuoaoefhuhfugm[.]to
aegohaohuoruitiiem[.]to	befaheaiudeuhughgm[.]to	sefuhsuifhishffo[.]ru
sefuhsuifhishfy[.]in	seiiamefiaigaefo[.]ru	seuufhehfueugheg[.]to
seuufhehfueugheh[.]ws	seuufhehfueughek[.]ws	seuufhehfueughem[.]top
seuufhehfueughet[.]to	sisfiusnrsruisfo[.]ru	sisfiusnrsruisy[.]in
sndiuenidniueifo[.]ru	soijodneoiauoefo[.]ru	wduufbaueeubffgh[.]ws

IP addresses

185[.]215[.]113[.]10	185[.]215[.]113[.]8	45[.]182[.]189[.]251
185[.]215[.]113[.]93	45[.]66[.]156[.]175	45[.]66[.]156[.]176
154[.]35[.]175[.]225	62[.]210[.]177[.]189	130[.]185[.]250[.]214
213[.]32[.]71[.]116	51[.]15[.]42[.]19	