Barkly

The Emotet Survival Handbook

Learn how to protect your company from 2018's most active threat

What is Emotet?

Emotet originally arrived on the scene as a new banking trojan in 2014. In the past 12 months, however, it has evolved from a standalone threat into a prolific distributor of other trojans, including TrickBot, Zeus Panda Banker, IcedID, Qakbot, and Dridex.

In 2018, it has become an increasingly pervasive menace, with the United States Computer Emergency Readiness Team (US-CERT) issuing an alert highlighting the serious threat posed by Emotet and describing it as "among the most costly and destructive malware" affecting organizations today.

What makes Emotet dangerous?

Because Emotet serves as a loader for other malware that means infections can result in a wide variety of repercussions and malicious activity that varies from campaign to campaign. Organizations infected with Emotet and the other trojans that it downloads may experience any of the following:

Emotet accounted for **57% of all banking trojan payloads** in Q1 2018.

Proofpoint Q1 2018 Threat Report

- **Persistent infections** designed to aggressively launch payloads at startup and at regular intervals, making remediation difficult
- **Credential theft,** including stolen network and email account credentials as well as any passwords stored in web browsers
- **Account lockouts** triggered by the malware's attempt to spread internally throughout the network via brute force attacks using stolen credentials
- **Disabled security tools,** specifically Windows Defender
- **Email hijacking** that occurs by scraping names and email addresses from the victim's Outlook account and then using the account to send out more malspam, essentially turning victims into spammers
- **Fraudulent bank account transfers or withdrawals** that result from banking trojans using webinjects to capture victim credentials and drain their accounts

Emotet and the other trojans it downloads are notorious for their persistence and self-propagating mechanisms, which can wreak havoc on networks and pose significant challenges for IT or incident response teams charged with remediation.

As an example, in March [the city of Allentown, PA was hit with an Emotet infection](#) that ran rampant through its network, forcing the closure of several public safety operations, putting a freeze on some of the city's financial transactions, and resulting in loss of access to certain law enforcement databases.

The city hired a team from Microsoft for an initial $185,000 emergency response fee, and estimated mitigation and recovery efforts would cost [an additional $800,000 to $900,000](#) before systems could be completely cleaned and restored.

Remediation efforts have cost up to $1 million per incident.

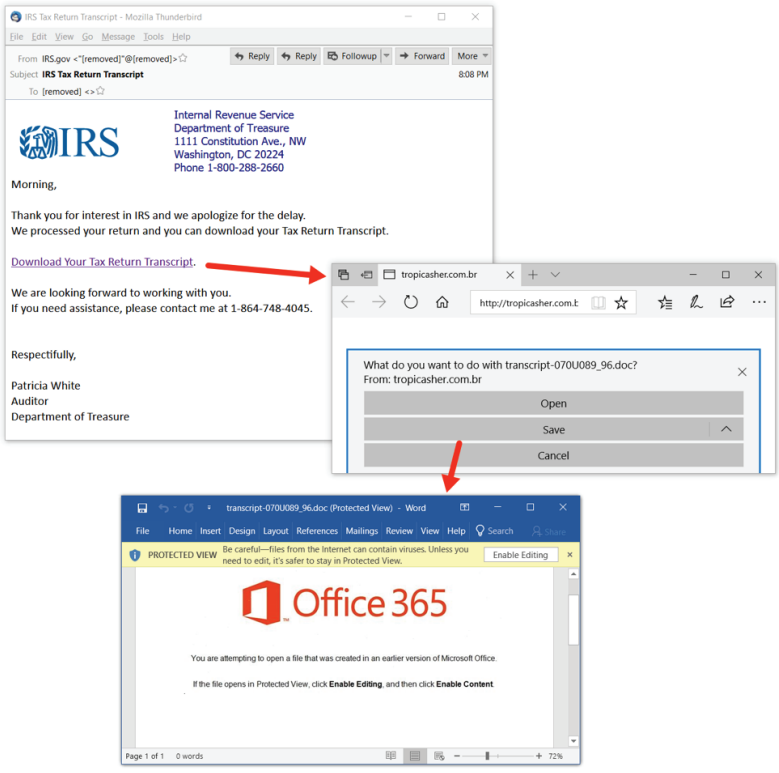
US-CERT

How is Emotet delivered?

Emotet campaigns are initially kicked off via malspam emails. In many cases, these emails tend to be in line with typical malspam themes (fake invoices, PayPal receipts, shipping notifications, etc.), but there are also examples of them being tailored to take advantage of specific occasions or events (ex: [IRS-themed, July Fourth-themed](#), etc.).

As part of its infection process, however, Emotet also hijacks victims' email accounts and uses them to deliver more malspam emails to addresses it finds in the victim's inbox and sent folders. This has been an extremely effective tactic for spreading the malware, as victims are much more likely to open emails from recipients they know and have previously corresponded with.

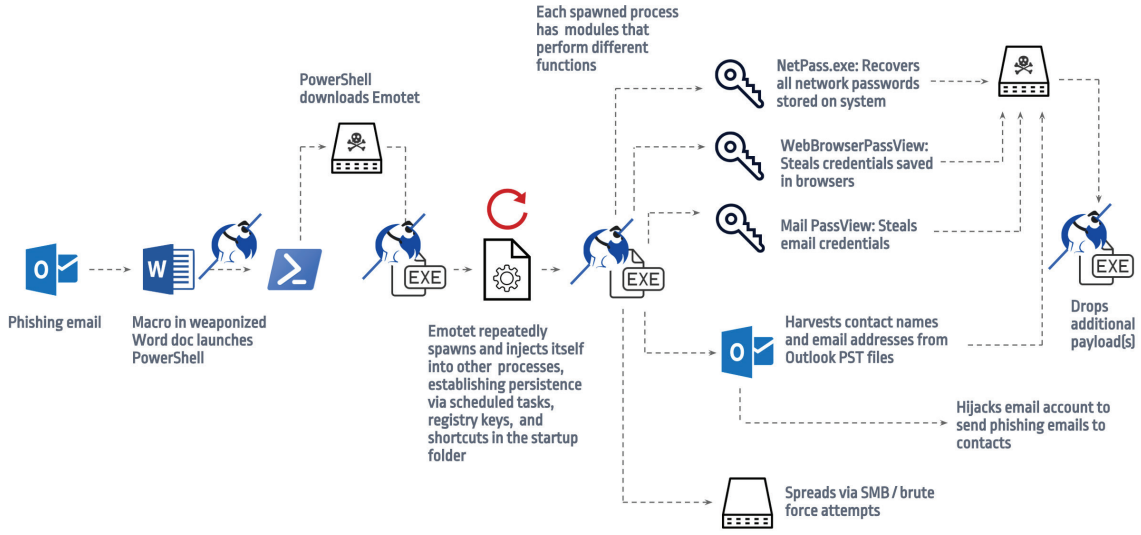
In addition to linking to malicious Word documents (as shown in the example above), Emotet campaigns also regularly attach malicious Word documents directly to emails. In either case, once opened, users are tricked into enabling macros in the Word documents in order to view them. Doing so launches the macro, which in turn launches PowerShell and downloads the Emotet payload.



Emotet malicious Word document distributed via link in IRS-themed email.
Source: [Brad Duncan](#)

How does Emotet work? Example attack diagram

Note: The diagram below depicts one of the many variations of Emotet infections in 2018. Emotet is constantly evolving, however, and current samples appear to have ditched the credential-scraping and self-propagation modules in favor of downloading and deploying other banking trojans with those capabilities.



Barkly provides defense in depth against Emotet by blocking infections at multiple points, including at the earliest possible opportunity — before the Emotet payload can even be downloaded.

Once Emotet has been retrieved, it begins deploying itself with two primary goals in mind: achieving persistence and spreading to more machines. We'll cover the various persistence mechanisms typically associated with Emotet infections in the next section below. To spread, Emotet and the banking trojans it downloads have been known to use a variety of self-propagation mechanisms. The specific mechanisms used at any one time can vary, but here is a list of typical capabilities and a few files in particular to look out for:

- **Network password scraper:** In the past, Emotet has used NetPass.exe, a legitimate utility that recovers all network passwords stored on the system for the current logged-on user. It can also recover passwords stored in credentials file of external drives.
- **Outlook PST scraper:** Collects names and email addresses from victim's Outlook account, uses them to send out more malspam from the victim's now-compromised account.
- **Browser password scraper:** Emotet has used WebBrowserPassView, another password recovery tool that captures passwords stored by Chrome, Internet Explorer, Firefox, Safari, and Opera.
- **Email account scraper:** Emotet has used Mail PassView, which reveals passwords and account details for popular email clients such as Outlook, Windows Mail, Gmail, Thunderbird, Hotmail, and Yahoo Mail.
- **Credential enumerator:** Self-extracting RAR file with two components. The first is a bypass component that enumerates network resources and attempts to gain access to additional machines by a) finding writable share drives using Server Message Block (SMB); or b) brute-forcing connections (in part using credentials gathered by tools listed above). The second is a service component that writes Emotet onto disk once any additional systems have been accessed.

This aggressive combination of persistence and self-propagation is what makes Emotet infections so damaging and painful to remediate. In worst case scenarios, one errant click from an end user can result in the infection of entire domains.

Think you may be infected with Emotet?

First things first:

DO NOT use privileged accounts to log in to potentially compromised systems during remediation. Doing so risks accelerating the spread of the infection.

Isolate any machines you suspect to be compromised by taking them off the network, and consider restricting inbound SMB communication between client systems by adjusting your firewall settings or using a Group Policy Object to set a Windows Firewall rule.

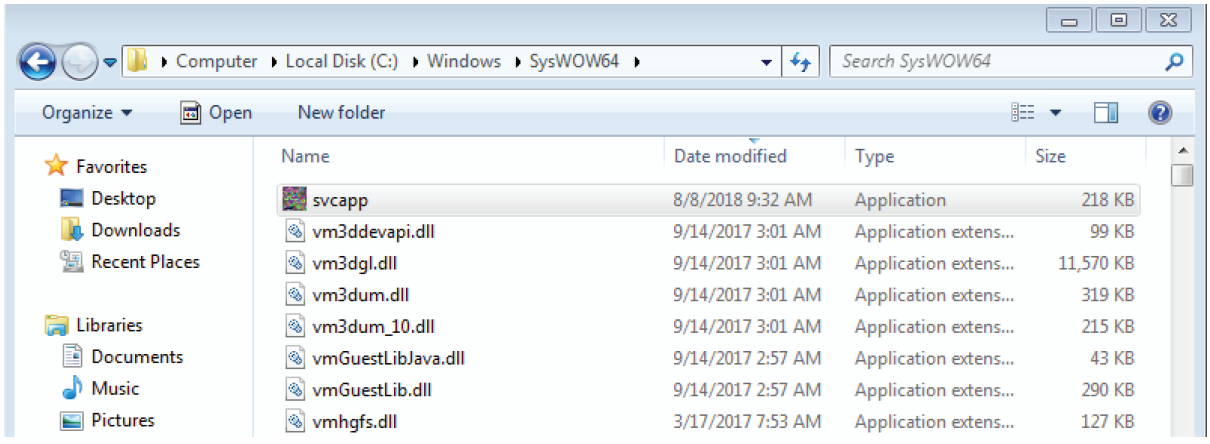
What to look for

With those initial steps taken, here are the different types of artifacts commonly associated with Emotet infections and where to go looking for them:

EXEs

- **Emotet typically stores executables in arbitrary paths** located off `AppData\Local` or `AppData\Roaming` directories (ex: `C:\Users\[username]\AppData\Local\Microsoft\Windows\[random].exe`). Because these payloads are polymorphic (each one is a modified mutation of previous samples), traditional antivirus solutions often have trouble detecting them. These files are also either randomly named or disguised with names mimicking legitimate executables (ex: flashplayer.exe), making detection difficult.
- **If Emotet gains admin privileges** it creates files in system root directories (ex: `C:\Windows\SysWOW64\svcapp.exe`) that are registered and run as Windows services. To blend in, these services may contain descriptions stolen from other legitimate services, but they typically don't list a publisher. Recent time stamps are other potential giveaways. To make things easier, look for the creation of new services by tracking Windows event ID 7045 in the system log.

Note: These services can also attempt to propagate via accessible admin shares.

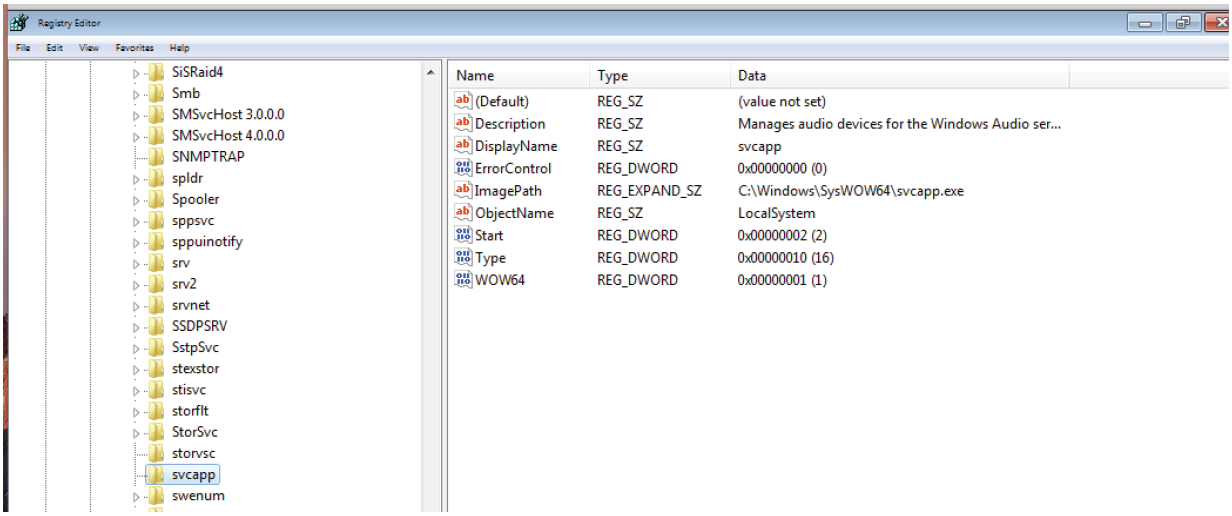


Emotet disguised as a new Windows service.

To verify maliciousness, you can upload any suspicious executables you find to VirusTotal or AnyRun.

Registry modifications

- Emotet typically creates a registry run key to ensure it gets executed at startup: `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\[random name of Emotet executable]`
- If it has admin privileges and has created a service, it creates the following registry subkey: `HKLM\SYSTEM\ControlSet001\services\[name of Emotet exe mimicking a service]`

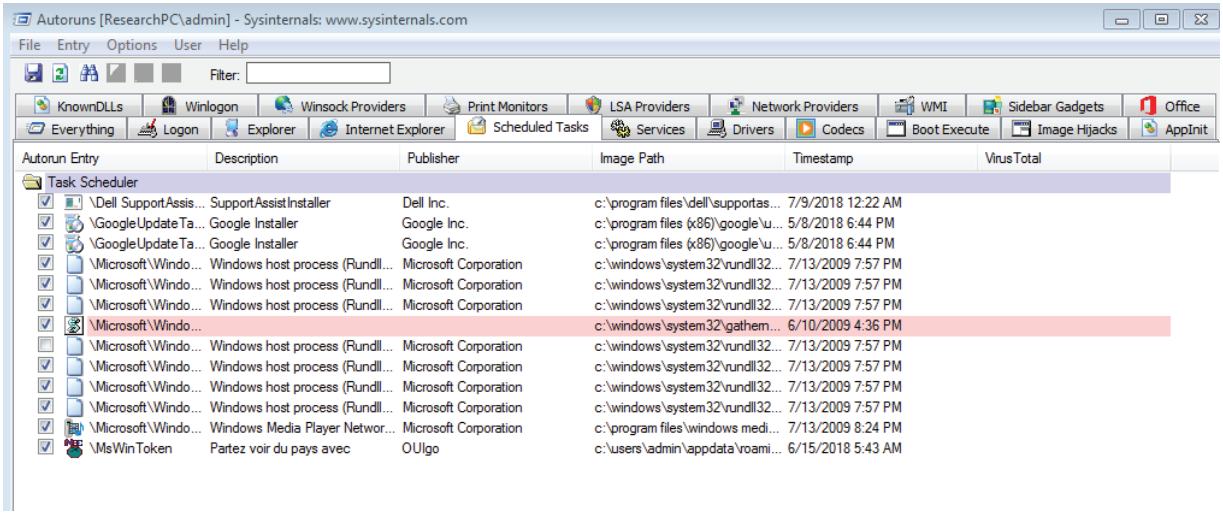


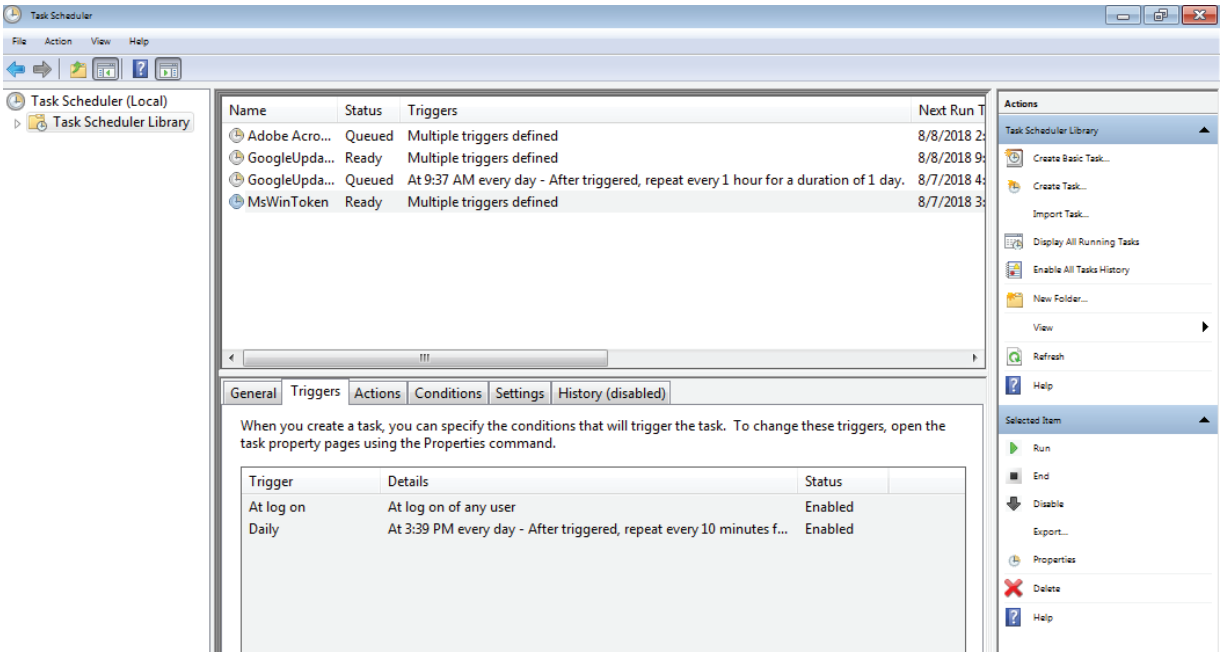
Using Windows Autoruns can help you investigate the registry and uncover whether any new or suspicious-looking programs are currently configured to auto-start. It also has VirusTotal integration, making it easy for you to verify whether suspicious programs are in fact malicious. Alternatively, you can find the most recent registry modifications by searching for Windows event ID 4657 in the system log.

You can also create a GPO to alert you to modifications to startup items in the registry.

Scheduled tasks

Current Emotet samples don't appear to be creating scheduled tasks to achieve persistence, but it's something the malware has done in the past and it's also a tactic the other banking trojans associated with Emotet (TrickBot, Zeus Panda, etc.) use frequently. Here is an example of a scheduled task created by Trickbot with triggers to run it at log on of any user and at regular intervals.





You can identify newly created scheduled tasks by using Autoruns, Task Scheduler, or by searching the Security log for Windows event ID 4698.

Warning: Change your passwords

Due to the credential harvesting and brute force attempts associated with Emotet infections it's a good idea to change all passwords associated with compromised machines, users, and accounts, including all local and domain administrator passwords. Email account passwords are especially important to change, otherwise victims can quickly find themselves turned into involuntary spammers with their accounts hijacked in order to send Emotet-spreading malspam to their contacts.

Bring cleaned machines back online slowly

Slowly reintroduce reimagined machines back onto the network but stay vigilant for signs of reinfection.

How Barkly can help

Barkly blocks Emotet infections before they have a chance to start. Barkly's unique protection provides customers with powerful defense in depth against Emotet:

- **Machine-learning-powered file analysis** blocks Emotet payloads regardless of whether they're new samples or polymorphic variations.
- **Behavior-based analysis** prevents malicious Office documents from retrieving the Emotet payload to begin with.

Dealing with an active Emotet infection?

Barkly prevents companies from getting infected with Emotet in the first place, but it can also help businesses battling with active infections by streamlining the incident response process.

- **Ensure all payloads are blocked** while you focus on remediation
- **Isolate compromised endpoints** with one click (even from your phone)
- **Investigate incident paths** to see where Emotet payloads are being launched from

Barkly can help.

Contact us to get started with a free consultation now.