Mitigating and eliminating info-stealing Qakbot and Emotet in corporate networks

cloudblogs.microsoft.com/microsoftsecure/2017/11/06/mitigating-and-eliminating-info-stealing-qakbot-and-emotet-in-corporate-networks/

November 6, 2017

The threat to sensitive financial information is greater than ever. Data breaches, phishing attacks, and other forms of information theft are all too common in today's threat landscape. Point-of-sale systems and ATMs have been targeted by hackers. Information-stealing trojans pose a risk to data and can lead to significant financial loss.

Qakbot and Emotet are information stealers that have been showing renewed activity in recent months. These malware families are technically different, but they share many similarities in behavior. They both have the ultimate goal of stealing online banking credentials that malware operators can then use to steal money from online banking accounts. They can also steal other sensitive information using techniques like keylogging.

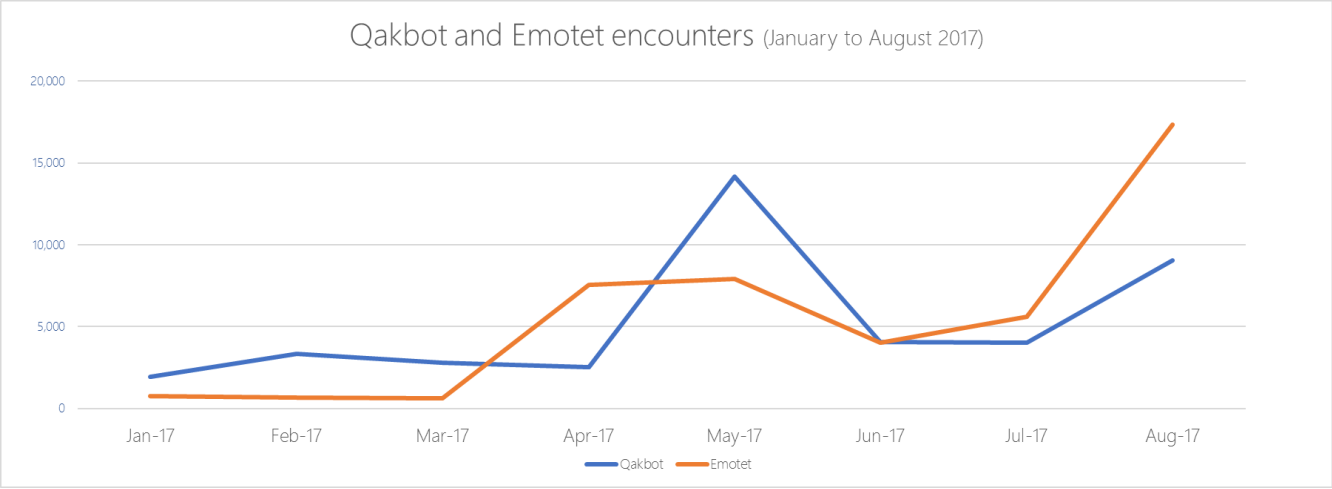


Figure 1. Qakbot and Emotet monthly machine encounters show an upward trend. This data doesn't include Qakbot and Emotet variants blocked by automation and cloud rules.

Even though these malware families are typically known to target individual online banking users, more and more enterprises, small and medium businesses, and other organizations have been affected by indiscriminate infections.

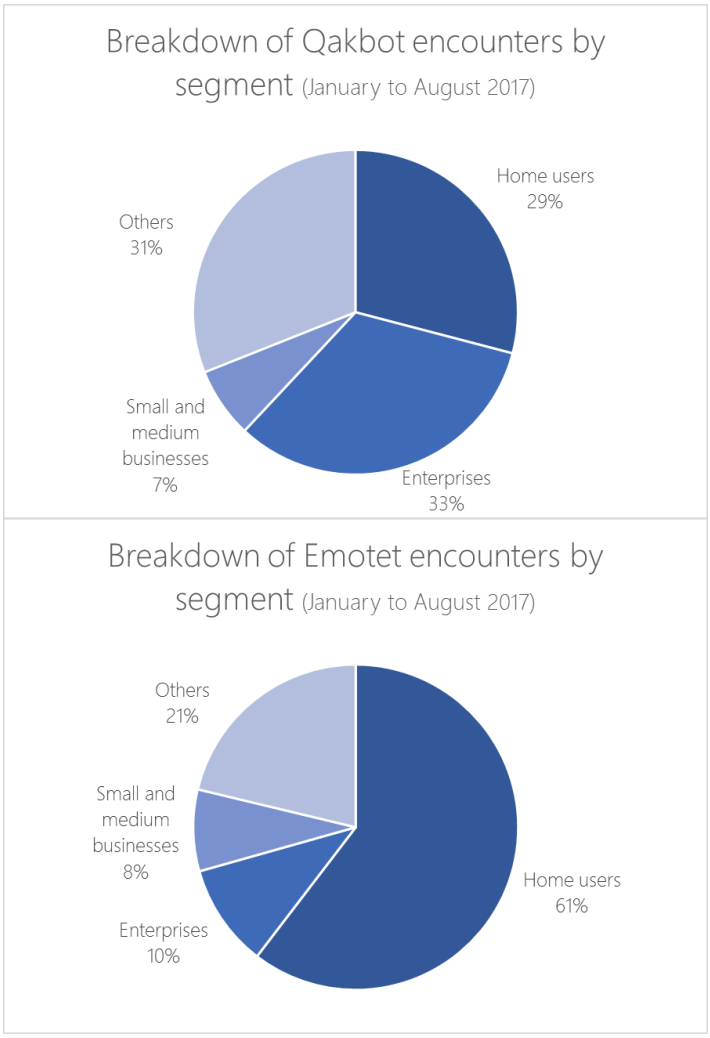


Figure 2. Breakdown of Qakbot and Emotet machine encounters

Recent variants of these malware families have spreading capabilities, which can increase the chances of multiple infections in corporate networks. They can also be spread by other malware during the lateral movement stage of a cyberattack.

Typical Qakbot and Emotet kill chain

Over the years, the cybercriminals behind Qakbot and Emotet have improved the code behind their malware. They have evolved to evade detection, stay under the radar longer, and increase the chances of spreading to other potential victims.

We mapped some of the common behaviors we've seen in Qakbot and Emotet variants and see a lot of similarities.

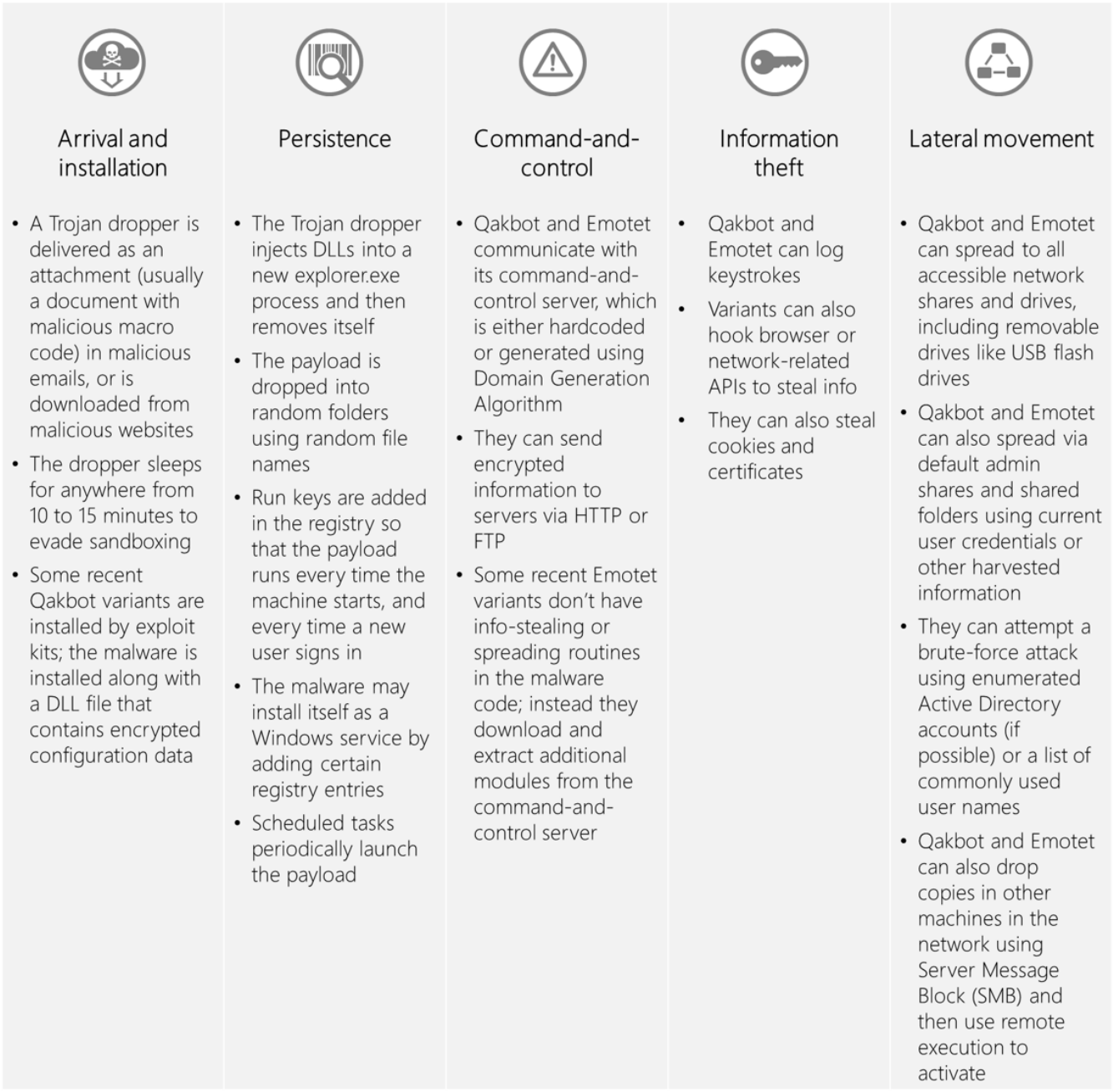


Figure 3. Qakbot and Emotet attack kill chain. Note that some Qakbot and Emotet variants might not exhibit all of the behaviors above and might be capable of unique routines.

Because of similarities in behavior, Qakbot and Emotet can be mitigated by similar security measures.

Steps to mitigate Qakbot and Emotet

Based on our experience helping organizations get rid of Qakbot and Emotet, the following steps mitigate infection and ultimately remove the said malware from corporate networks:

1. **Stop the spread of malware and cut off communication with its command-and-control server**

    - Cut off Internet access or disconnect the affected machines from the network until they have been cleaned. Windows Defender Advanced Threat Protection customers can isolate affected machines with one click. You can also block infected machines at the edge firewall, unplug machines from the network, or create rules on Windows Defender Advanced Firewall (and push these out via Group Policy Objects (GPO)).
    - Stop sharing folders that show signs of infection or set shared folders to read-only. Removing admin shares is an option that should only be used as a last resort as this can cause other issues and hinder management
    - Practice credential hygiene. Remove unnecessary privileges, or disable privileged accounts that have been observed to spread malware using SMB.

2. **Look for new service creations and scheduled tasks**

    - Look for new service creations by tracking event ID 7045 in the system log. We've observed this threat to create services with randomly generated number strings as the name and .exe name, but cleans them up after.
    - You can look for new scheduled tasks using even ID 106 in the task schedule log or 7045 to track down machines.

3. **Remove Qakbot, Emotet, and other related malware**

    - Obtain and submit samples to your antivirus vendor. Malware samples can be obtained by following the scheduled tasks and reviewing the target binaries. For Microsoft customers, use the Windows Defender Security Intelligence submission portal.
    - Deploy updated definitions as soon as your antivirus vendor has tested and released them. Enable cloud-delivered protection to get the latest protection in real-time. Do a full scan on all affected machines. For Windows Defender Antivirus customers, learn how to manage updates.
    - Uncover undetected variants by inspecting infected systems for scheduled tasks and their target binaries. The Sysinternals Autoruns tool can be your friend here. Windows Defender ATP customers can review the timeline of known affected machines to find undetected malware components. Additional affected machines can be identified by reviewing the incident graph for the relevant alert or by searching for threat known artifacts, such as file SHA1s, IP addresses, and URLs.

4. **Monitor the network for possible reinfection**

    - Determine and address the initial attack vector. Use security solutions like Windows Defender ATP, which provides detailed timelines and other contextual information to understand the nature of attacks and take response actions.
    - Slowly reintroduce network connectivity to the subset of the machines that have been cleaned. Monitor them for reinfection.
    - Reintroduce network connectivity to all affected machines that are believed to be clean.
    - Turn on real-time protection in your antivirus. In Microsoft Security Essentials and Windows Defender Antivirus for Windows 10, enable cloud-based protection and automatic sample submission. With these features enabled, Windows Defender Antivirus provides advanced real-time protection against never-before-seen threats.

Preventing Qakbot and Emotet infections with Windows 10

While the steps above can rid networks of Qakbot and Emotet, preventing infection eliminates opportunities for these threats to steal info. Windows 10 S is a streamlined platform with Microsoft-verified security. It blocks malware like Qakbot and Emotet and other malicious programs by working exclusively with apps from the Windows Store, ensuring that only apps that went through the Store onboarding, vetting, and signing process are allowed to run.

Additionally, Windows 10 has a comprehensive defense stack that can help block and detect malware like Qakbot and Emotet.

Use Microsoft Edge to block Qakbot and Emotet infections from the web. Microsoft Edge opens pages within low privilege app containers and uses reputation-based blocking of malicious downloads. Its click-to-run feature for Flash can stop malware infections that begin with exploit kits. With Windows Defender Application Guard, Microsoft Edge has an additional hardware isolation-level capability on top of its exploit mitigation and sandbox features.

Block malicious emails carrying trojan droppers that install Qakbot and Emotet using Microsoft Exchange Online Protection (EOP), which has built-in anti-spam filtering capabilities that help protect Office 365 customers. Secure mailboxes against email attacks with Office 365 Advanced Threat Protection, which blocks unsafe attachments, malicious links, and linked-to files leveraging time-of-click protection. Outlook.com anti-spam filters also provide protection against malicious emails.

Enable Windows Defender Exploit Guard to block malicious documents (such as those that use macro code to install Qakbot and Emotet, or the more recent DDEDownloader that install other malware) and scripts. The Attack Surface Reduction (ASR) feature in Windows Defender Exploit Guard uses a set of built-in intelligence that can block malicious behaviors observed in malicious documents. ASR rules can also be turned on to block malicious attachments from being run or launched from Microsoft Outlook or webmail (such as Gmail, Hotmail, or Yahoo).

Use Credential Guard to protect domain credentials and help stop malware from spreading using compromised credentials.

Use Local Administrator Password Solution (LAPS) to manage local account passwords and domain joined computers.

Enable Windows Defender AV to detect Qakbot and Emotet variants, as well as all related malware such as droppers and downloaders. Windows Defender AV uses precise machine learning models as well as generic and heuristic techniques and enhanced behavior analysis to detect common and complex malware code. It provides advanced real-time protection against new and unknown files using the Windows Defender AV cloud protection service.

Use Windows Defender Advanced Threat Protection to flag Qakbot or Emotet infections and to enable security operations personnel to stop the spread of these threats in the network. Windows Defender ATP's enhanced behavioral and machine learning detection libraries flag malicious behavior across the malware infection process, from delivery and installation, to persistence mechanisms, command-and-control communication, and lateral movement. The new process tree visualization and improvements in machine isolation further help security operations to investigate and respond to attacks.

To test how Windows Defender ATP can help your organization detect, investigate, and respond to advanced attacks, **sign up for a free trial**.

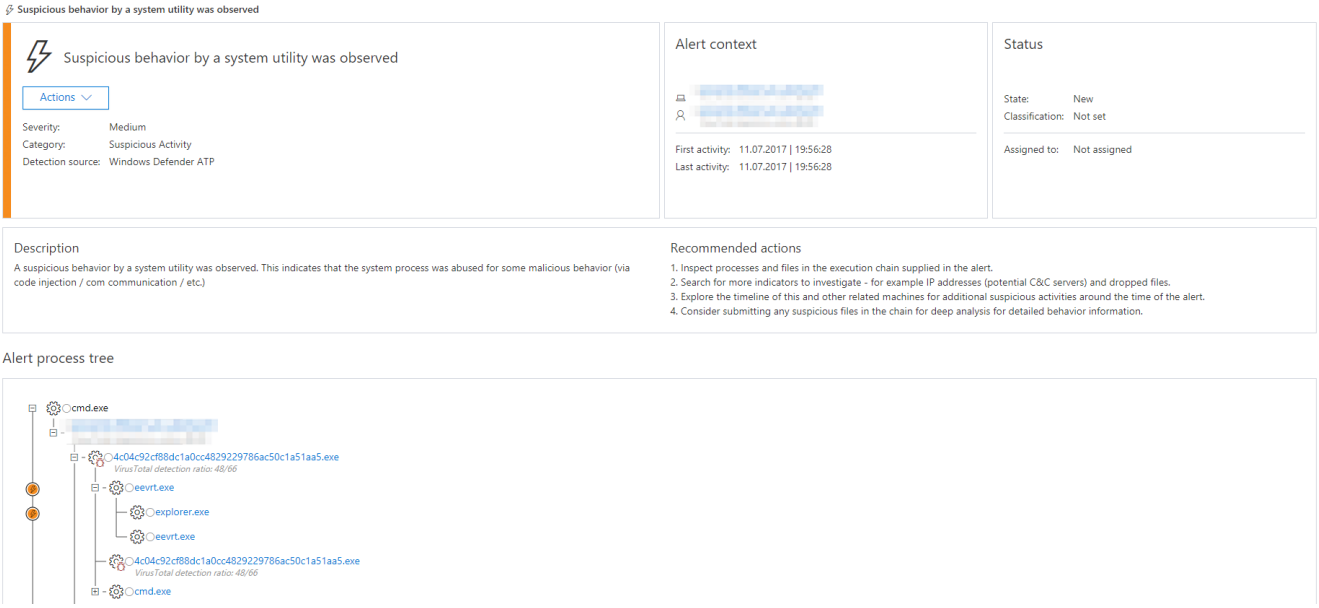


Figure 4. Machine learning-based alert in Windows Defender ATP showing suspicious memory injections and registry modifications

These end-to-end security features in Windows 10 help defend against increasingly complex malware attacks. At Microsoft, we continue to harden Windows 10 against attacks. With Fall Creators Update, we shipped several new and enhanced security features that make Windows 10 the most secure version of Windows yet. Learn more about these features:

It is also important for organizations to augment these security technologies with a security-aware workforce. Educating employees on social engineering attacks and internet safety, and training them to report suspicious emails or websites can go a long way in protecting networks against cyberattacks.

***Keith Abluton**, Windows Escalation Services*

***Rodel Finones**, Windows Defender Research*

Indicators of compromise

The following are IOCs for recent Qakbot and Emotet variants:

Qakbot

Qakbot malware (SHA256):

da00823090dae3dae452ddc8a4c2a3c087389b4aacf1f0c12d13c83c9fcaef9c

ca2d536b91b15e7fc44ec93bbed1f0f46ae65c723b8a4823253a2a91b8241f9a

Filenames:

%APPDATA%\Microsoft\<random folder name>\<random file name>, for example:

%APPDATA%\Microsoft\Cexpalgxx\Cexpalgxx.exe

%APPDATA%\Microsoft\Cexpalgxx\Cexpalgxx32.dll (configuration file)

Registry modifications:

In subkey: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Sets value: <random value name>

With data: “%APPDATA%\Microsoft\<random folder name>\<random file name>”

In subkey: HKLM\SYSTEM\CurrentControlSet\services\<random service name>

Sets value: ImagePath

With data: “%APPDATA%\Microsoft\<random folder name>\<random file name> /D”

Sets value: Type

With data: dword:00000010

Sets value: “Start”

With data: dword:00000002

Sets value: “DisplayName”

With data: “Remote Procedure Call (RPC) Service”

Sets value: “ErrorControl”

With data: dword:00000000

Sets value: “DependOnService”

With data: “Dnscache”

Sets value: “ObjectName”

With data: “LocalSystem”

In subkey: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Sets value: ctfmon.exe

With data: “%APPDATA%\Microsoft\<random folder name>\<random file name>” /c “%System Folder%\ctfmon.exe”

Command-and-control servers:

64.183.173.170:995

67.213.243.228:993

96.67.244.225:443

173.25.234.18:443

24.123.151.58:443

76.164.161.46:995

68.115.254.146:443

198.57.88.73:443

47.21.79.34:443

174.51.185.121:465

71.3.55.80:993

88.244.177.127:443

180.93.148.41:443

101.51.40.175:443

73.166.94.110:443

71.88.202.122:443

74.5.136.50:990

89.43.179.209:443

211.27.18.233:995

96.82.91.67:443

98.194.132.179:443

98.113.137.220:443

24.184.200.177:2222

105.224.247.34:443

Emotet

Emotet downloader (SHA256):

4ce5366c7eef1fff1260d5d7a0aec72c1246621838bf8df07f4a6ab3e5369d96

Emotet malware (SHA256):

ffcb204da3ff72d268c8ac065c2e7cce5c65fafc2f549d92d0c280c6099bd440

59639027a7fd487295bad10db896528ea223684e6595cae4ce9a0bec8d809087

Filenames:

%appdata%\roaming\microsoft\windows\start menu\programs\startup\[random].lnk

%Appdata%\local\[random]\[random].exe

%localappdata%\microsoft\windows ex: C:\Windows\System32\netshedule.exe

Registry modifications:

In subkey: ‘HKLM\SYSTEM\ControlSet001\services\netshedule’ <Bug: 5667568 Type & Size>

Sets value: ‘Type’

With data: ‘0x00000010’

In subkey: ‘HKLM\SYSTEM\ControlSet001\services\netshedule’ <Bug: 5667568 Type & Size>

Sets value: ‘Start’

With data: ‘0x00000002’

In subkey: ‘HKLM\SYSTEM\ControlSet001\services\netshedule’ <Bug: 5667568 Type & Size>

Sets value: ‘ErrorControl’

With data: ‘0x00000000’

In subkey: ‘HKLM\SYSTEM\ControlSet001\services\netshedule’ <Bug: 5667568 Type & Size>

Sets value: ‘ImagePath’

With data: ‘C:\Windows\system32\netshedule.exe’

In subkey: ‘HKLM\SYSTEM\ControlSet001\services\netshedule’ <Bug: 5667568 Type & Size>

Sets value: ‘DisplayName’

With data: ‘netshedule’

Command-and-control servers:

104.236.252.178

162.243.159.58

45.33.55.157

77.244.245.37

192.81.212.79

173.212.192.45

103.16.131.20

195.78.33.200

50.116.54.16

212.83.166.45

137.74.254.64

104.227.137.34

188.165.220.214

85.143.221.180

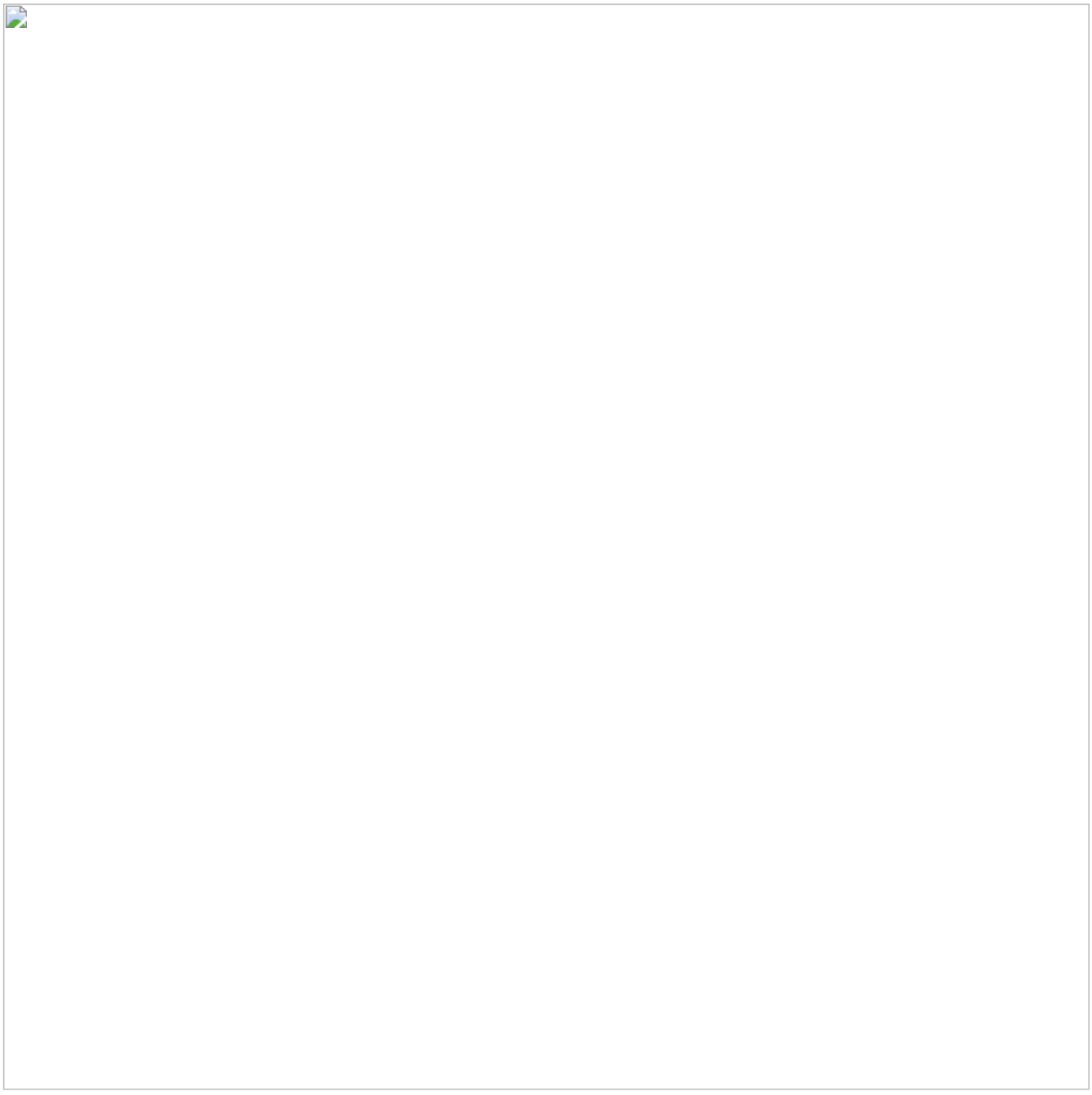
119.82.27.246

194.88.246.7

206.214.220.79

173.230.136.67

173.224.218.25



Talk to us

Questions, concerns, or insights on this story? Join discussions at the Microsoft community and Windows Defender Security Intelligence.