SOPHOS

Emotet: Nastier Than WannaCry and Harder to Stop

Emotet is an exceptionally nasty, destructive threat causing huge problems for organizations around the world. This fast-moving, ever-changing malware uses multiple advanced techniques to get through your defences – which means it requires the very best defenses to stop it.

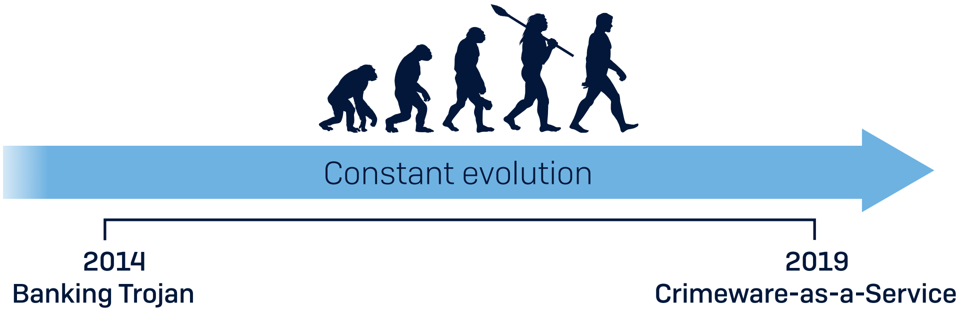
This paper will help you understand what Emotet is, how it works, and why it's so very, very dangerous. We'll also explain how Sophos gives you the very best protection against Emotet at every point in the attack chain, as well as the three best practice steps that every organization should follow to minimize their risk of being hit by Emotet.

Understanding Emotet

Emotet is a very sophisticated worm. In fact, the U.S. Department of Homeland Security considers it to be among the most costly and destructive threats to U.S. businesses right now. Not that it limits itself to the U.S. – more on that in a moment.

The U.S. Department of Homeland Security considers it to be among the most costly and destructive threats to U.S. businesses right now[1]

Emotet is not a new piece of malware, but it's one that's become steadily more complex and destructive over the years. Emotet first appeared on the scene five years ago, starting off as a Trojan that silently stole banking credentials. Since then it has evolved into a highly-sophisticated platform for distributing other kinds of malware. It's Crimeware-as-a-Service personified.



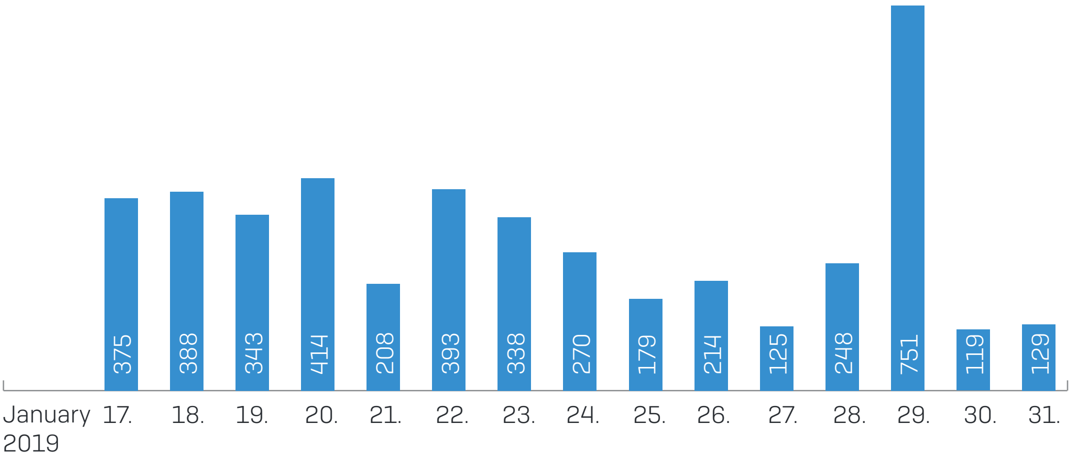
Emotet serves up whatever malware pays. So far in 2019 that's meant TrickBot and QBot banking Trojans, although it's also been linked with BitPaymer, a strain of sophisticated ransomware that extorts six-figure payouts.

The people behind Emotet are highly professional and financially motivated. They continuously update their malware to make it ever more powerful and destructive.

Constantly-changing payloads

One of the characteristics of Emotet is that its payloads change all the time. This graph shows the number of new unique Emotet payload executables seen by SophosLabs in the last two weeks of January 2019.

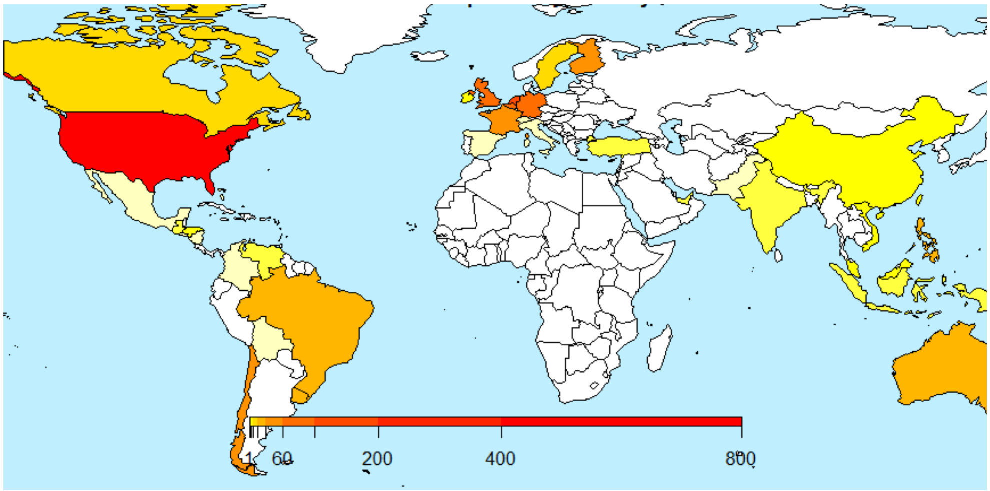
# of unique Emotet payload executables seen by SophosLabs



As you can see, there are literally hundreds of versions daily. In fact, on average, SophosLabs sees around 300 new, unique payload executables every day, and saw almost four and a half thousand (4,494) unique payload executables in the last 15 days of January alone.

Global reach

While the U.S. Department of Homeland Security rates Emotet as one of the most costly and destructive threats around, Emotet doesn't limit itself to the U.S. This visual here from SophosLabs shows the countries hit worst by Emotet – the closer to red, the greater the number of attacks.

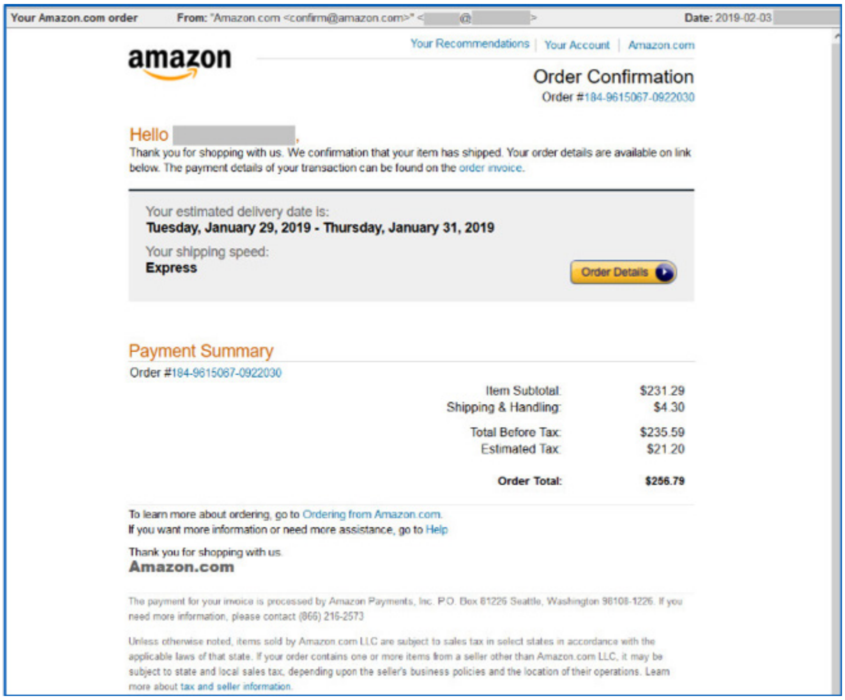


Geographic coverage of Emotet. Source: SophosLabs

While SophosLabs sees Emotet in almost all regions, North and South America, Northern and Western Europe, Turkey, Australia, South East Asia, China, India, and Pakistan are all very popular targets. Africa and Eastern Europe are currently less targeted, but don't let this lull you into thinking you don't need to worry in these regions. The cybercriminals behind Emotet are quick to take advantage of new opportunities and we don't know where they will go next.

It starts with spam

Emotet generally arrives on the back of a spam campaign. The emails encourage you to click on a malicious document. Emotet spam began as emails with malicious document attachments but have since evolved into emails with links to malicious documents hosted on websites. Social engineering and brand spoofing is a common feature of Emotet spam, with Amazon, PayPal, and AT&T some of the common brands used.



Your Amazon.com order **From:** "Amazon.com <confirm@amazon.com>" <[redacted]@[redacted]> **Date:** 2019-02-03 [redacted]

Order Confirmation

Order #184-9615067-0922030

Hello [redacted],

Thank you for shopping with us. We confirmation that your item has shipped. Your order details are available on link below. The payment details of your transaction can be found on the order invoice.

Your estimated delivery date is:
Tuesday, January 29, 2019 - Thursday, January 31, 2019

Your shipping speed:
Express

Payment Summary

Order #184-9615067-0922030

Item Subtotal:	$231.29
Shipping & Handling:	$4.30
Total Before Tax:	$235.59
Estimated Tax:	$21.20
Order Total:	**$256.79**

To learn more about ordering, go to Ordering from Amazon.com.
If you want more information or need more assistance, go to Help

Thank you for shopping with us.
Amazon.com

The payment for your invoice is processed by Amazon Payments, Inc. P.O. Box 81226 Seattle, Washington 98108-1226. If you need more information, please contact (866) 216-2573

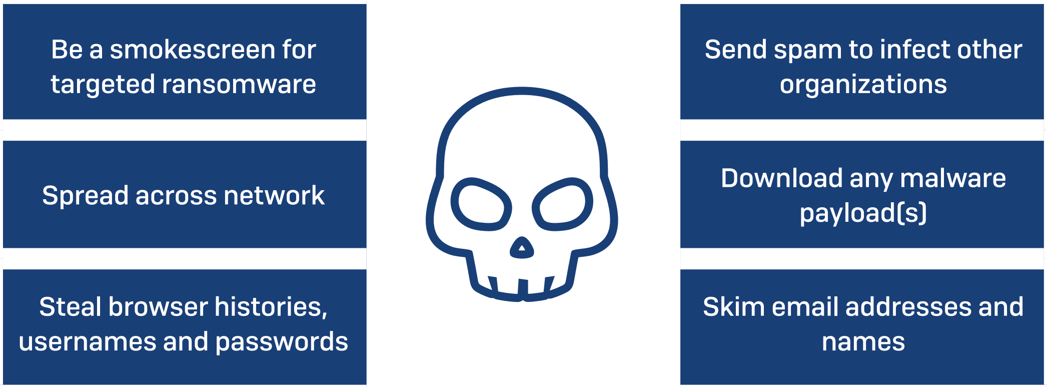
Unless otherwise noted, items sold by Amazon.com LLC are subject to sales tax in select states in accordance with the applicable laws of that state. If your order contains one or more items from a seller other than Amazon.com LLC, it may be subject to state and local sales tax, depending upon the seller's business policies and the location of their operations. Learn more about tax and seller information.

Example of Emotet spam email. Source: SophosLabs

Emotet's (many) goals

When it comes to what Emotet does, unfortunately the answer is 'lots of things.' Once inside your computer, Emotet tries to:

1. **Spread onto as many machines as possible.** It's a worm, so can spread without user interaction. It moves from one infected computer to another via the network.
2. **Send malicious emails** to infect other organizations.
3. **Download a malware payload.** Traditionally the payloads have mostly been banking Trojans, with TrickBot the most prevalent. Its payload injects code into your browser to automatically debit your bank and PayPal accounts when you next log in.
4. Some Emotet variants **skim email addresses** and names from email client data and archives, likely so they can be sold as part of a wider list and used to spread more malicious spam.
5. Others inspect your web browser, **stealing histories and saved usernames and passwords.**
6. To add to the pain, Emotet can also be a **smokescreen for targeted ransomware attacks**. While organizations are dealing with Emotet infections, ransomware like BitPaymer takes advantage of the distraction to hold the organization's data hostage.



Be a smokescreen for targeted ransomware

Spread across network

Steal browser histories, usernames and passwords

Send spam to infect other organizations

Download any malware payload(s)

Skim email addresses and names

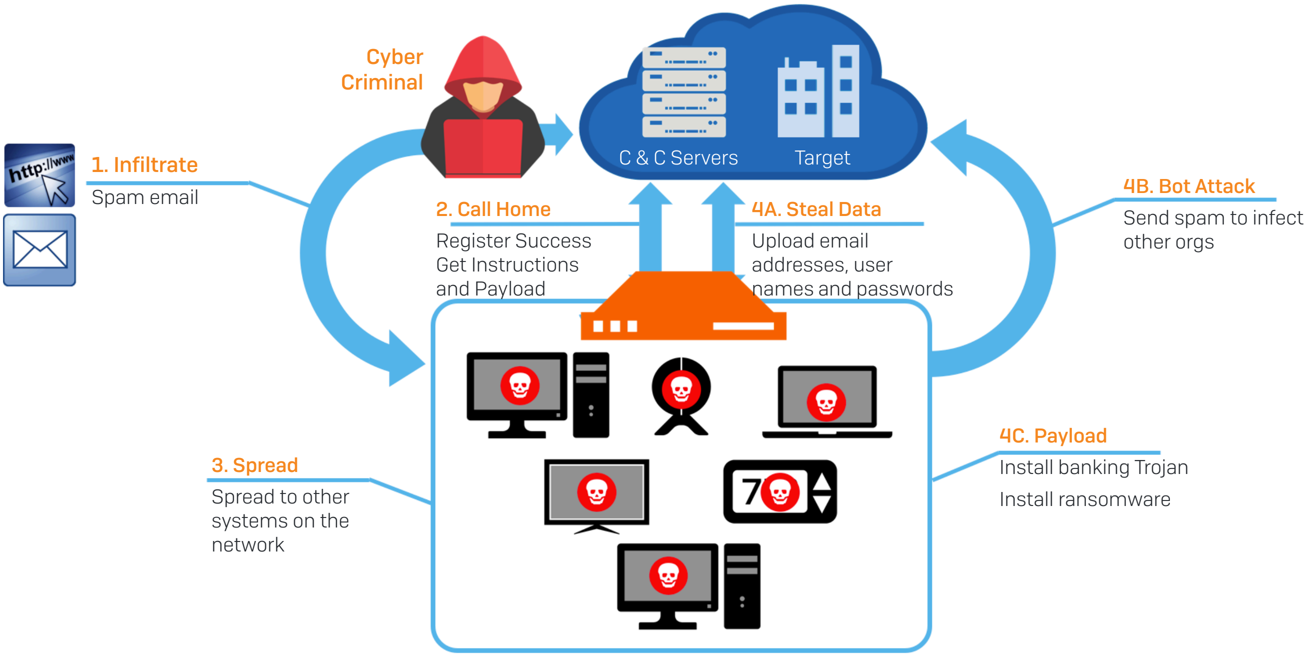
Emotet's activities are hugely damaging for impacted organizations. Repercussions include:

- The financial and operational costs of the banking Trojan
- Sender reputation damage because of distributing malicious spam
- The costs and compliance implications of a data breach from lost contact information
- The security breach from the loss of user names and passwords
- Potentially, the financial costs of targeted ransomware attack

Its therefore no surprise that Emotet infections have cost U.S. governmental organizations up to **US$1 million per incident to remediate.**[2]

Defending against Emotet with Sophos

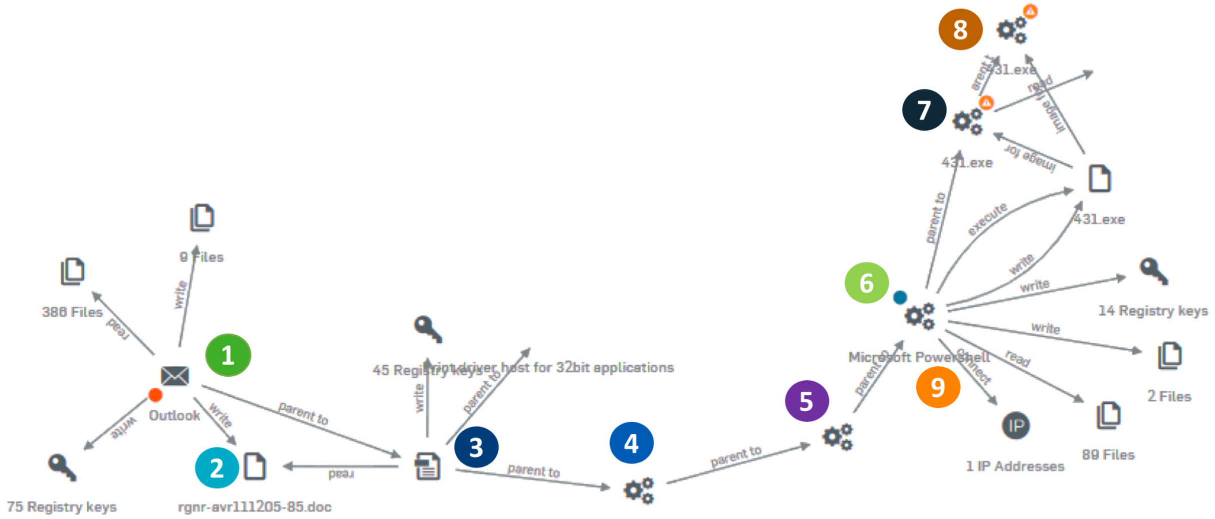
To secure against a sophisticated threat like Emotet you need the very best advanced protection technologies. That's exactly what Sophos delivers, at both the endpoint and the network. To understand how to protect against Emotet, it's important to understand how the attack works.



Sophos protects against Emotet in multiple ways at every point in the attack chain, from stopping the threat entering your network in the first place, to preventing it spreading to other parts of the network. This blocks it from calling home and stealing data, and stops it installing its payloads.

Stop Emotet from infecting your endpoints

Emotet performs multiple actions on the endpoint to carry out its attack, as you can see in the below example attack chain from January 2019.



1. User receives a malicious email (malspam).

2. User clicks on a malicious attachment: a document called rgnr-avr111205-85.doc

3. User enables malicious macros in the document.

4. The macro uses CMD (Command Prompt) to execute malicious obfuscated code.

5. CMD launches a second copy of CMD.

6. The second copy launches Microsoft PowerShell.

7. PowerShell connects to an IP address and downloads a file called 431.exe

8. PowerShell executes 431.exe

9. Sophos HIPS detected PowerShell connecting to a suspect IP address and downloading an exe with unkown reputation, and blocked this behaviour.

Intercept X Advanced with EDR is packed with technologies to prevent Emotet from delivering its payload. It delivers the multiple layers of protection you need to secure against such a fast-moving, sophisticated threat as Emotet.

- **Delivery.** Web protection stops the delivery of the malicious email.
- **Exploitation.** Anti-exploit (code/ memory/ APC) mitigations, application lockdown, local privilege mitigation and application control, all stop the exploit executing.
- **Installation.** Deep learning and HIPS block the installation of malware.
- **Command and Control.** Malicious Traffic Detection (MTD) stops communication with the C&C server, preventing the threat from getting instructions.
- **Action on Objective.** Anti-ransomware and credential theft protection, runtime HIPS, and RCA all stop Emotet from carrying out its goals.

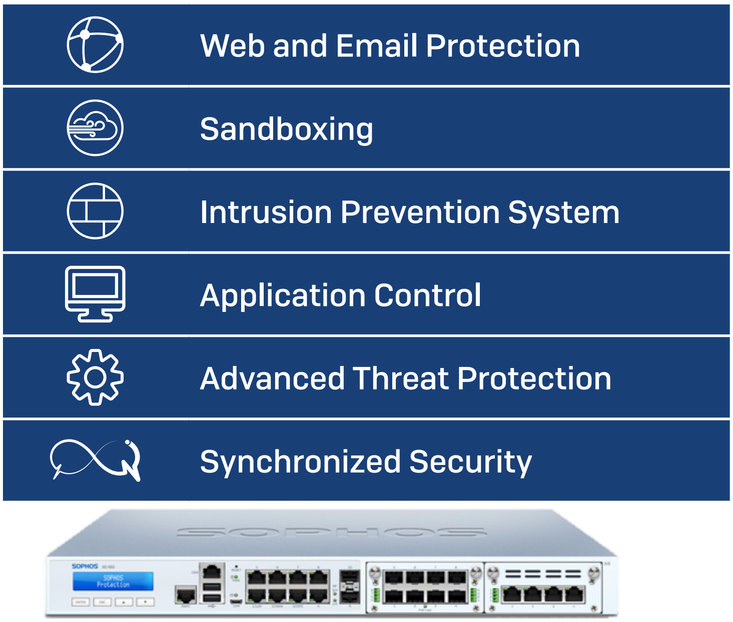
With a threat that changes and evolves as quickly as Emotet, it's essential to be able to predict what's coming next and block variants that have never been seen before. The deep learning capabilities in Intercept X does exactly that, anticipating new threats before they are released. We don't know what Emotet will look like next week or next month, but predictive technology that blocks unseen threats gives you the best possible future-proofing.

EDR or endpoint detection and response is an important part of effective Emotet defenses. As we've seen, Emotet is not your common garden variety malware. It's highly persistent. The EDR capabilities in Intercept X allow you to answer the tough questions:

- What happened?
- What did it touch?
- Did we lose any data?
- Are there any sleeper threats?

Stop Emotet from getting on your network

When it comes to stopping Emotet getting on your network in the first place, there's no such thing as a "silver bullet". XG Firewall includes a full suite of protection technologies that all play an important role in defending against Emotet and together give you the best possible defenses. Plus everything's managed from a single screen in a firewall rule, so you can easily see the security you have applied to any particular connection or traffic type.



Web and Email Protection

Sandboxing

Intrusion Prevention System

Application Control

Advanced Threat Protection

Synchronized Security

Email protection blocks both inbound and outbound Emotet spam, leveraging SophosLabs threat intelligence to identify malicious emails.

Sophos Sandstorm sandboxing gives you your best protection from zero day and emerging file-based threats. Emotet droppers are a perfect example of the kinds of threats Sandstorm is designed to identify. Sandstorm has the best technology from Intercept X working in the virtual sandbox in the cloud – technology like exploit detection, anti-ransomware, and deep learning.

In the case of Emotet, Sandstorm will identify:

- Emotet memory signatures
- malicious behavior in office documents associated with Emotet
- malicious use of PowerShell
- attempts to connect with high-risk URLs
- and, of course, any overt malicious behavior

One of the benefits of Sandstorm is that it can run more aggressively than a typical endpoint analysis because it doesn't care about user performance – and it's extremely effective.

Intrusion Prevention (IPS) should also be a foundational element of your network defenses. IPS is the network equivalent of exploit detection. It looks at network traffic for signs of exploits, or any packet containing code that's part of an attack.

Sophos IPS can detect exploits against vulnerabilities in operating systems, network stacks, servers, endpoints, browsers, applications, and more. For example, TrickBot, a common payload dropped by Emotet, uses the same SMB vulnerability as WannaCry to spread throughout networks and that is easily detected and blocked by IPS.

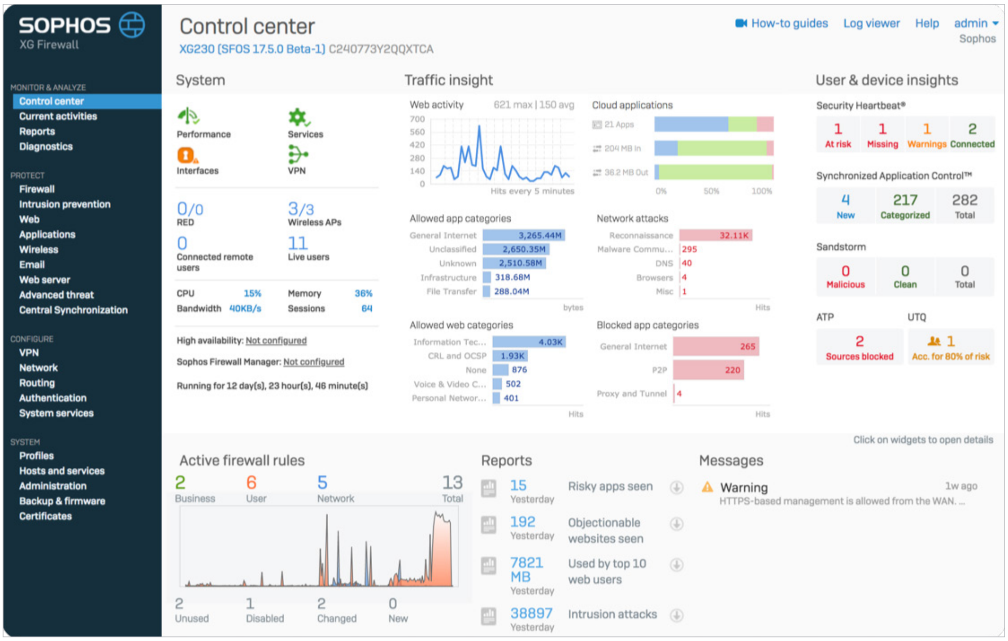
IPS is particularly helpful in situations where an unmanaged endpoint is brought onto the network with some kind of infection that then starts trying to reach out to other systems on the network.IPS will identify and block those attempts.

The Sophos IPS engine is among the best in the industry, ranking in the top three for security effectiveness and performance in recent NSS Labs testing.

Stop Emotet from communicating and stealing data

XG Firewall also includes technologies to help prevent a threat like Emotet from stealing data or communicating out. The Advanced Threat Protection (ATP) capability monitors all traffic leaving the firewall for signs that it's communicating with malware servers, command and control servers, or hacker systems and instantly identifies the machine and threat.

Our enormous database of known hacker and C&C servers is maintained by SophosLabs and continuously updated via Live Cloud to ensure we're able to identify even the latest variants of threats like this attempting to call home. This saves enormous time in identifying where you have a threat, while also enabling you to clean it up quickly.



Control center

XG230 (SFOS 17.5.0 Beta-1) C240773Y2QQXTCA

High availability: Not configured

Sophos Firewall Manager: Not configured

Running for 12 day(s), 23 hour(s), 46 minute(s)

Warning 1w ago
HTTPS-based management is allowed from the WAN. ...

Elevate your Emotet Protection with Synchronized Security

Intercept X protects your endpoints against Emotet, and XG Firewall secures you at the network level. Individually, they offer the best protection around. Together they take protection to a whole new level – one that no other vendor comes close to. We call it Synchronized Security.

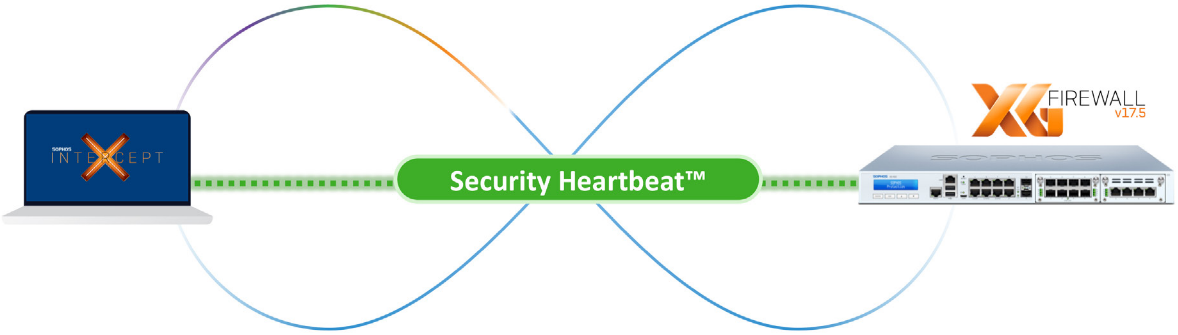
With Synchronized Security, Sophos products work together to identify and contain threats like Emotet. It's all done automatically, zero-touch, in seconds. Intercept X and XG Firewall share real-time security information via a Security Heartbeat™ and automatically respond thanks to dynamic policies in the Firewall.

Zero-touch Emotet Response

1 **Malware Detection**
Intercept X detects Emotet running

2 **Cross-Estate Communication**
Intercept X tells XG Firewall on which machines it's detected Emotet

3 **Device Isolation**
XG Firewall instantly isolates the Emotet-infected machines.
- Isolated from outside world
- Isolated from other endpoints



4 **Clean-up**
Intercept X automatically cleans up the infection. Once Emotet is removed, Intercept X shares this update with XG Firewall

5 **Access Restored**
XG restores network access. Guided investigations provide a detailed view of what happened

If Intercept X detects Emotet, it alerts XG Firewall, which then instantly isolates the machine – both from the outside world and also from other endpoints, even if they are on the same network segment or switch, preventing lateral movement.

It also works the other way round: if XG Firewall detects Emotet or one of it's payloads like TrickBot through IPS or ATP, it will inform the endpoint and automatically isolate the infected machine directly. Either way, you get an instant indicator on the XG Firewall control center identifying the machine, user, and even process and threat – automatically, without having to do anything.

Best practices to block Emotet

Secure ALL of your machines.	Patch early. Patch often.	Block PowerShell by default.

Best practices work hand in glove with your protection technologies to secure your organization from Emotet. Sophos recommends that everyone follows these three steps:

1. Secure ALL of your machines

Unknown, unsecured machines give Emotet a place to hide and adapt, making a bad situation much worse. Although Emotet may currently be confined to the unsecured machine by the security software on your other machines, it will be trying to break free all the time. And because it's updated so often it's continuously presenting new challenges. The longer it's allowed to run through those machinations, the greater the risk that an update to Emotet, or a change of payload, will find a gap in your armor that allows it to break out and spread through your network.

Run a network scan tool (such as Advanced IP Scanner) and check that you don't have any unprotected machines on your network. Many organizations have discovered Emotet nesting in a machine that they weren't even aware of, and so hadn't protected.

2. Patch early, patch often

This may feel like the oldest advice under the sun, but that doesn't make it any less important. Emotet is a gateway for other malware, so containing an Emotet outbreak doesn't just mean stopping Emotet, it means stopping whatever it brings with it. Since you don't know what that will be, you have to take the best bang-for-your-buck precautions you can, and that means patching known vulnerabilities.

EternalBlue is the exploit made famous in 2017 by WannaCry and NotPetya. Despite all the headlines, and almost two years since Microsoft released patches to protected against it, TrickBot – the payload most commonly delivered by Emotet – is still making profitable use of this exploit.

3. Block PowerShell by default

As we saw in the attack chain earlier, Emotet attacks typically use PowerShell. We recommend that you begin with the assumption that nobody needs it (including admins) and then unblock it just for the people who really do need PowerShell to perform their jobs. And be sure to block PowerShell, not just set a policy to disable it. Policies can be bypassed, so PowerShell should be blocklisted. (Within Sophos products, the functionality that does this is Application Control).

Conclusion

Emotet is a formidable foe that leaves a trail of devastation in its wake. To stop a threat of this nature you need advanced defenses at every point in security infrastructure. Sophos gives you the best possible Emotet defenses with:

- Proven advanced protection at the endpoint and firewall
- Unique zero-touch threat isolation and clean-up with Synchronized Security
- Deep learning technologies to mitigate the risk from future Emotet evolution

By combining Sophos' advanced protection technologies with best practices techniques you give yourself the possible protection against Emotet.

To learn more about Sophos products and take them for a test drive visit www.sophos.com

[1] U.S. Computer Emergency Readiness Team
[2] https://www.us-cert.gov/ncas/alerts/TA18-201A

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS