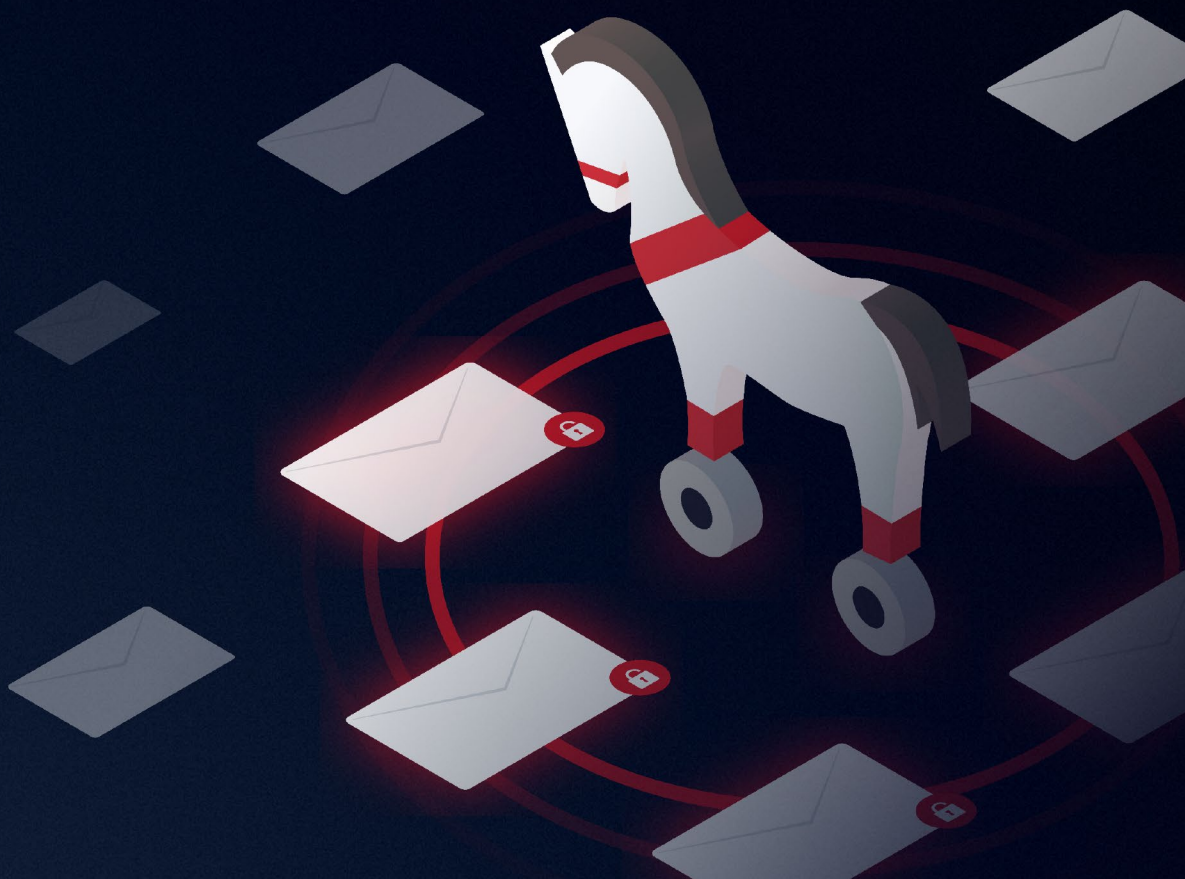
VARONIS

WHITEPAPER

Emotet Battle Plan: Prevent, Detect & Recover with Varonis



Introduction

Our incident response team is tracking an unprecedented number of Emotet malware infections. The number of active concurrent Emotet investigations is threefold our previous high-water mark. This paper will cover indicators of compromise, mitigations, and how Varonis can help you detect and stop Emotet at each phase of an attack.

Emotet Overview

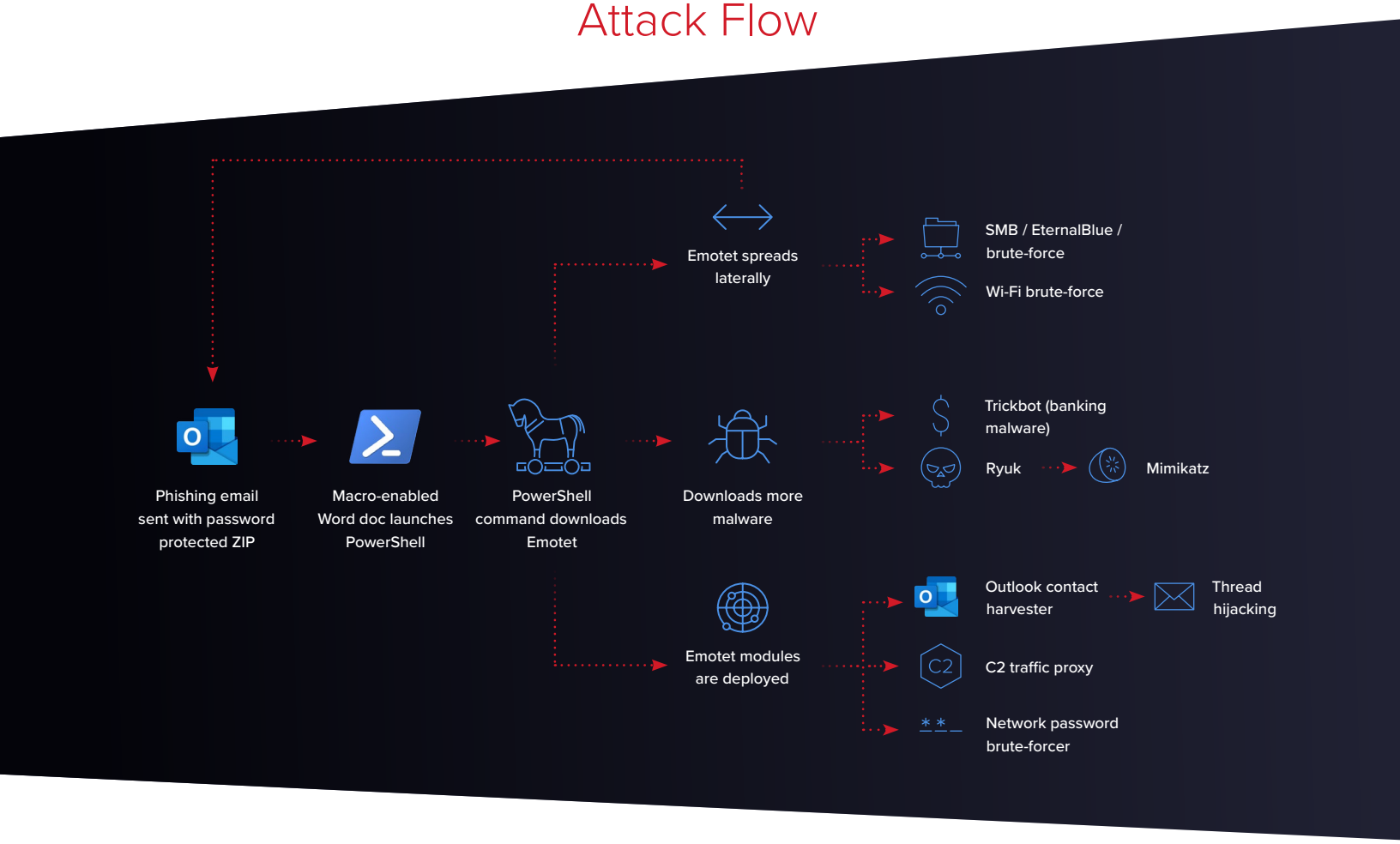
After a long break during the spring of 2020, the threat actor TA542 (a.k.a. “Mummy Spider”) is back with a massive new malspam campaign powered by multiple worldwide botnets and powerful new malware functionality.

Emotet, originally known as a banking trojan, was first seen in the wild in 2014. Its primary goal was to intercept banking credentials via man-in-the-browser attacks. Emotet has evolved into a self-updating, general purpose suite of malware that also acts as a loader for payloads such as **Qbot** and Trickbot (which in turn loads Ryuk and Mimikatz for a nice Russian doll effect).

Because Emotet is polymorphic, the specific IOCs — such as loader URLs, C2 IP/port combos, and spam templates — change frequently. This makes rule-based detection a cat-and-mouse game compounded by the fact that there are three different Emotet botnets, each with their own supporting infrastructure. You can find a wonderfully detailed **daily log of Emotet IOCs** maintained by the Cryptolaemus Team.

Once inside a network, Emotet has various methods for moving laterally, escalating privileges, establishing persistency, and exfiltrating data. Luckily, Varonis’ behavioral-based threat models can detect early signs of compromise by Emotet as well as post-intrusion behavior.

Attack Flow



VARONIS

Initial Compromise

Emotet's infection vector of choice is phishing email powered by three global botnets called Epoch 1, Epoch 2, and Epoch 3 (or E1, E2, E3 for short). Epochs have their own C2 infrastructure, update schedules, and malspam templates. Spam from a given Epoch will contain macro-enabled attachments or malicious links designed to infect new hosts and add new spammers to its cluster.

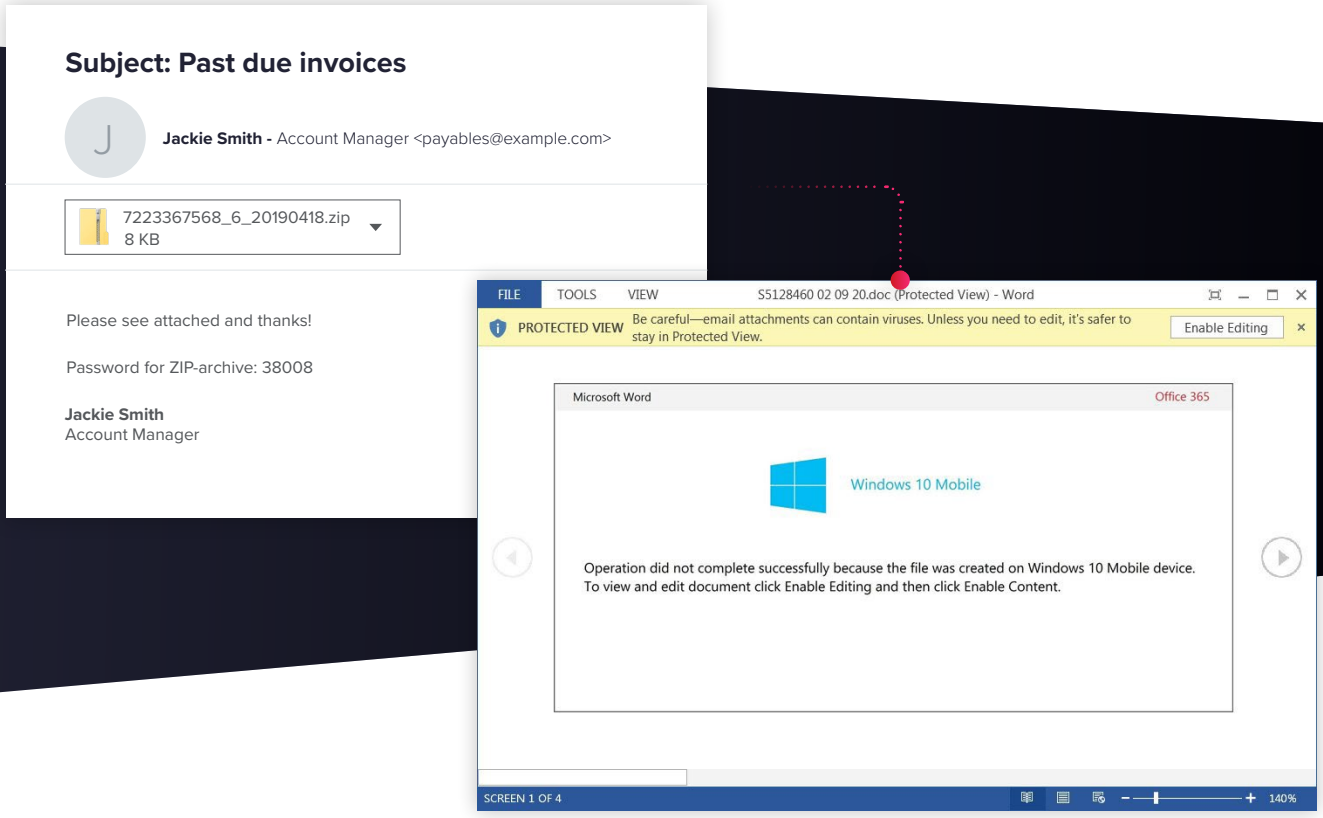
In the latest wave of infections, Emotet malspam email contains password-protected ZIP attachments. The hope is that email filters won't be able to scan and detect the malicious macro-enabled documents within the archive. This has been dubbed "Operation Zip Lock."

The password is usually included in the body of the email in plain text, e.g.,:

```
Zip file attached to email: Very urgent
information from 24-09-2020.zip
The password for the document is LQWMFXu
```

Given the surge in ZIP attachments, it's a good idea to quarantine emails with password-protected archives. Keep in mind, however, that Emotet uses directly attached Office documents, too.

Malspam campaigns have been detected in many languages: English, Dutch, French, German, Italian, Japanese and Epochs appear to be geographically assigned (e.g., E3 has been hammering Japan).



VARONIS

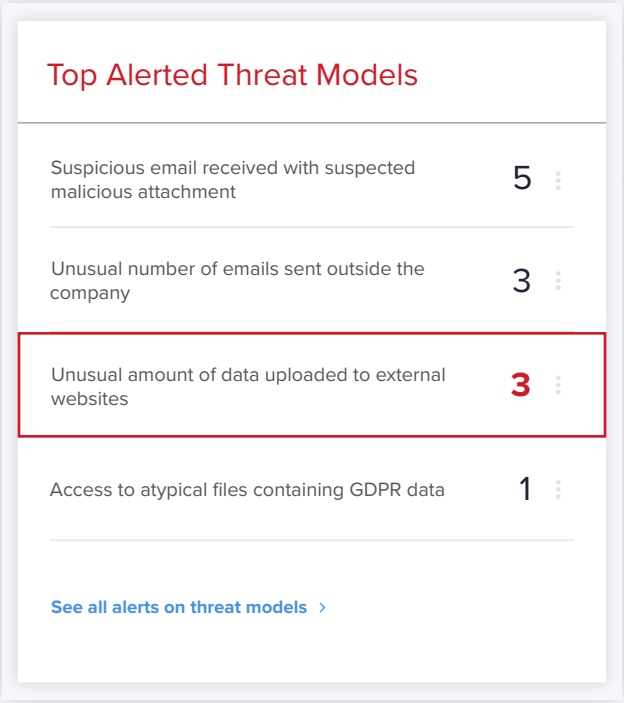
Thread Hijacking

Emotet steals victims' email messages and contact lists via HTTP POST requests back to the C2 server. The botnet then uses stolen email data to impersonate the sender and "reply" to existing conversations. They can do this either by spoofing the sender or, if they have full control over the victim machine, by sending the email directly from the trusted party.

This technique makes Emotet spam appear legitimate and increases the likelihood that a new victim will open a malicious attachment.

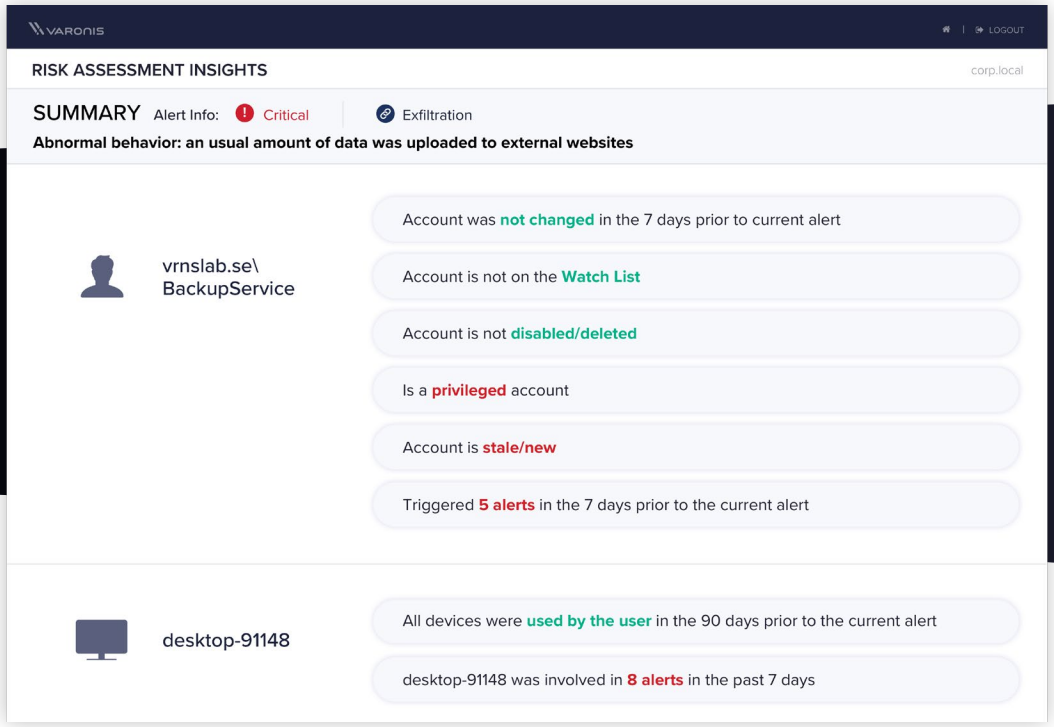
Varonis monitors Microsoft Exchange and Exchange Online mailboxes and can detect malicious file attachments that match a dictionary of known patterns used in Emotet spam templates. With Edge's proxy-based detections, customers can also detect when a user clicks on a link within the body of an email that results in a malicious Emotet loader download.

Varonis analyzes all mailbox actions (send/receive/open/delete, etc.) to quickly identify accounts that are compromised and have begun sending spam campaigns (internally or externally). A user's behavior profile is built across multiple platforms — subtle deviations in email behavior combined with suspicious logon events, network connections, and data access produce high-fidelity alerts with few false positives.



Varonis Edge can detect actions such as exfiltration of email messages and Outlook contacts. We've observed email and contact harvesting primarily via proxy monitoring — Emotet has been using HTTP POST commands for exfiltration — but if a more covert DNS channel is established in the future, Edge has DNS-based exfiltration models covered as well.

Unusual connections back to the C2 servers can be detected in several ways. First, if a connection is to a domain with a poor reputation, Varonis will alert on and tag these connections. Second, Varonis detects when attackers hide their traffic in lots of connections ("white smoke") using a domain generation algorithm (DGA). Third, Varonis' behavioral models will also detect when attackers use DNS as a covert channel to hide their commands or data transfers as queries. Lastly, Varonis will alert on unusual web activity, such as the use of new or unusual user agents[1], unusual or first-time access to the internet by an account, or unusual upload activity.



Varonis uses machine-learning to detect when a user's upload/download activity deviates from their historical norm.

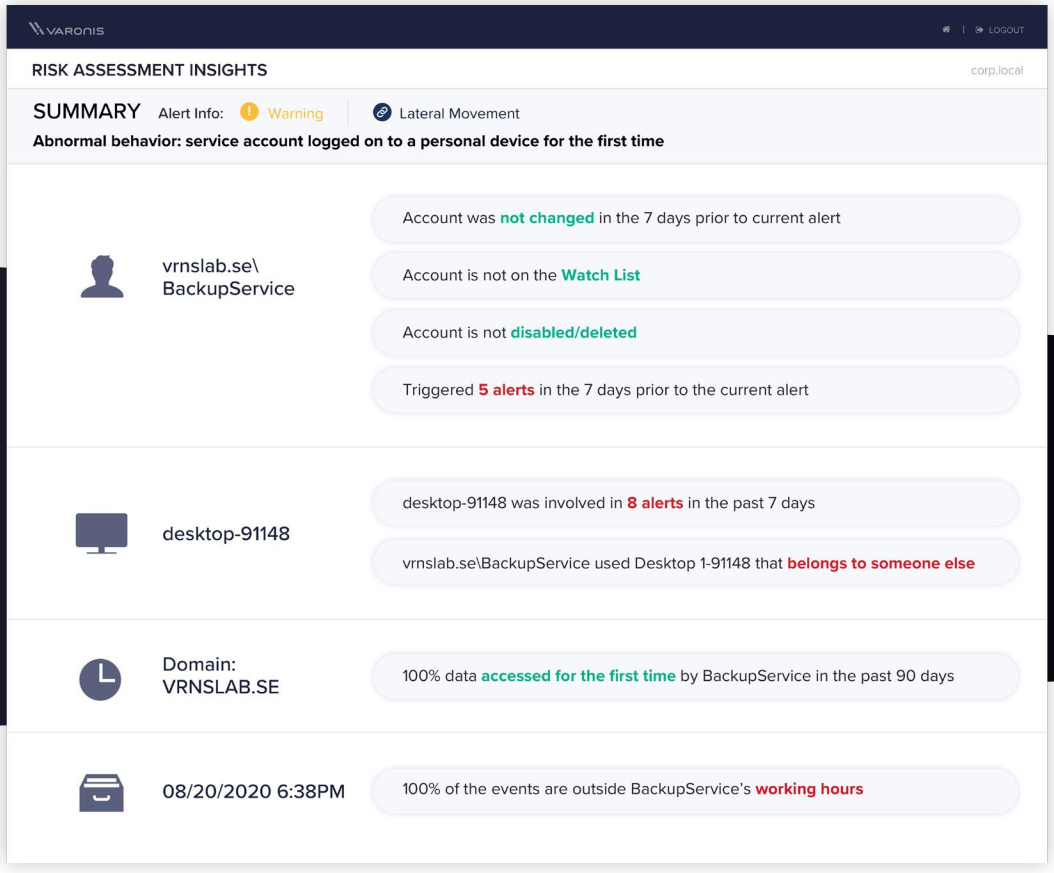
1 A user agent is a string sent from the web client to the web server that identifies the browser and OS version.

Lateral Movement

Emotet has an array of modules, or plugins, that can be loaded dynamically from its C2 server to extend the malware's functionality. There's a spam-sending module, an email-stealing module, a banking module, etc. You can think of it like adding a new app to your phone.

One module to pay special attention to is the lateral movement module which enables spreading via SMB exploits like EternalBlue **(MS17-010)** and by accessing hidden admin shares (ICP$, C$, and Admin$). We recommend patching any machines that are still vulnerable to EternalBlue and **disabling admin shares.**

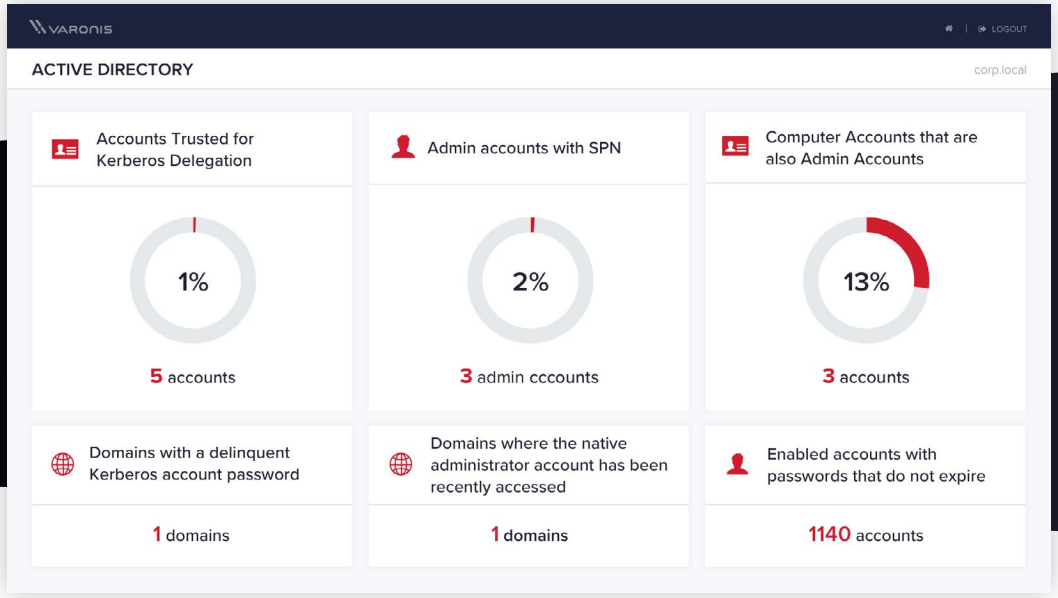
While the main method Emotet spreads is via SMB, the malware will also try to brute-force nearby Wi-Fi networks and spread to the computers that connect to them.



Because Varonis tracks the associations between users and the devices and resources they access, threat models will detect on an unusual number of connections made by an account, connections made to systems not normally accessed, as well as brute-force attempts like password sprays and credential stuffing.

Privilege Escalation

Attackers obtain credentials to privileged accounts by using well-known open-source tools, looking for passwords stored in plain text, and harvesting credentials from Active Directory. Once administrative credentials are obtained, the attacker may add one or more users to a domain administrator group and upload credentials to cloud storage services.



By watching file system activity, Varonis quickly detects when known penetration tools are saved to disk, or when a user searches file shares for files with passwords or other sensitive data. Any given user account typically has access to far more data than they should, so these searches are frequently fruitful — more on mitigating this below.

Emotet is well-known for loading other strains of malware such as Ryuk, which then loads hacking tools such as Mimikatz to harvest credentials and escalate privileges. Varonis analyzes Active Directory activity to detect credential harvesting (e.g. Kerberoasting) and other attacks. To reduce the chances that these attacks will be successful, Varonis highlights potential targets (e.g. administrative accounts that are associated with a Service Principal Name (SPN)) in a dashboard — reducing the attack surface in AD and on file systems helps make ransomware groups' jobs more difficult. Varonis will also alert when an account is added to an administrative group.

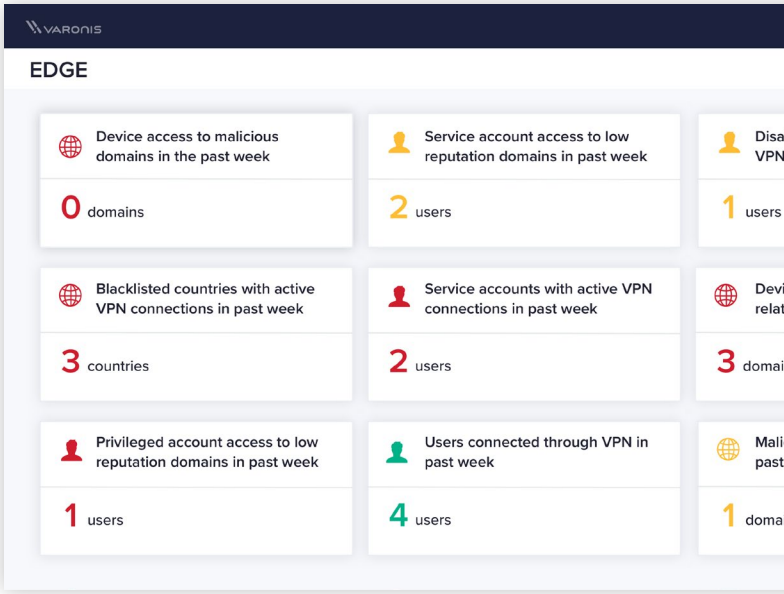
As above, should any of these accounts connect to the internet for the first time, connect to low-reputation domains, or generate unusual upload activity, Varonis will alert on these signals.

Endgame

If signs of initial compromise, lateral movement and privilege escalation are missed, Varonis provides a critical layer of defense around your largest data stores, protecting Windows and UNIX servers, NAS devices, SharePoint and Exchange (both on-prem and in Microsoft 365).

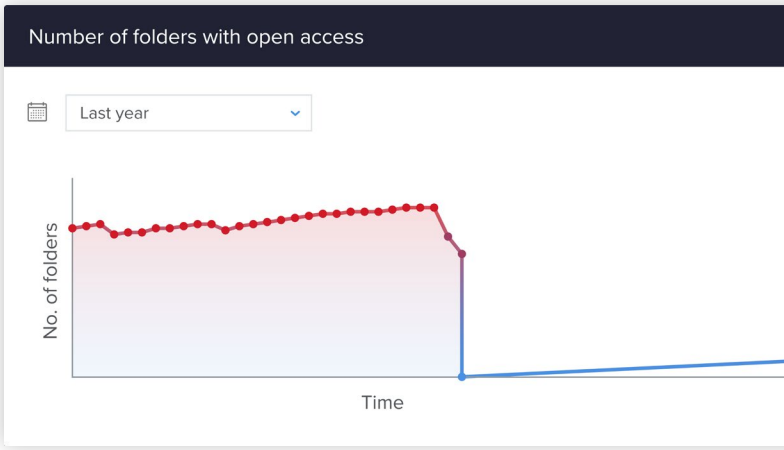
Varonis captures more information about how users interact with data than any other technology — it analyzes file system activity on platforms that provide adequate auditing through their API's, like Microsoft 365 and NAS devices from NetApp and EMC. Where native auditing is lacking, like Windows, UNIX, Exchange, and SharePoint, Varonis uses battle-tested filesystem filters to capture file operations.

If a user starts to access an unusual amount of data compared to its normal behavior, Varonis will detect this with one or more of its many behavioral models (as well as detecting unusual uploads, as mentioned above). If a user starts to encrypt files, this will also be detected — many customers automate responses to this kind of behavior, disabling the account and killing active connections.



Varonis also reveals where data is overly accessible and where users or groups have access they don't need and automates processes to lock it down. Restricting access to important data will reduce overall risk surface area and make any threat actor's job more difficult.

With a detailed, searchable log of all file system access, it's much quicker to assess and recover from damage. Instead of searching through directories for ransom notes, you can run a query for all the file accesses and modifications made by any user over any time period to pinpoint affected files, and then restore the correct versions.



Removing Global Access groups immediately reduces risk.

Conclusion

Emotet's botnet is the world's largest and most sophisticated weapon for spreading malware. It's difficult to predict what TA542 will use this weapon for next or which APTs will rent their weapon. What we do know is that Emotet campaigns occur in bursts and vary greatly in nature, so it's extremely important to have a multi-layered approach to defense including patch management, anti-phishing training, mail filtering, endpoint detection, and data-centric security.

Sophisticated detection can give your organization an edge — so can reducing the overall attack surface. Varonis' data-centric technology starts from the inside out, building out rings of detective controls from the data, to Active Directory and DNS, to VPNs and proxies. Varonis also highlights vulnerable accounts and data so you can lock them down before attackers exploit them. These controls can help protect your organization from any threat actor — from the casual insider to the advanced, persistent sorts we're dealing with too frequently these days.

Complimentary Incident Response Service

If you're under attack, or just looking for some help to understand what you're seeing, call on the expertise of our Incident Response team. They'll help you investigate and resolve any incident, whether you're a Varonis customer or trial user.

Try Varonis free

Set up Varonis in your own environment. Fast and hassle free.

info.varonis.com/demo

ABOUT VARONIS

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data on premises and in the cloud: sensitive files and emails; confidential customer, patient and employee data; financial records; strategic and product plans; and other intellectual property.

The Varonis Data Security Platform detects insider threats and cyberattacks by analyzing data, account activity and user behavior; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation. With a focus on data security, Varonis serves a variety of use cases including governance, compliance, classification, and threat analytics. Varonis started operations in 2005 and has thousands of customers worldwide — comprised of industry leaders in many sectors including technology, consumer, retail, financial services, healthcare, manufacturing, energy, media, and education.