Stolen emails reflect Emotet's organic growth

By Jaeson Schultz

Published: 2020-01-16 · Archived: 2026-04-05 21:31:05 UTC

Thursday, January 16, 2020 09:00

By Jaeson Schultz

Introduction Emotet has a penchant for stealing a victim's email, then impersonating that victim and sending copies of itself in reply. The malicious emails are delivered through a network of stolen outbound SMTP accounts. This relatively simple email-man-in-the-middle social

engineering approach has made Emotet one of the most prolific vehicles for delivering malware that we have seen in modern times.

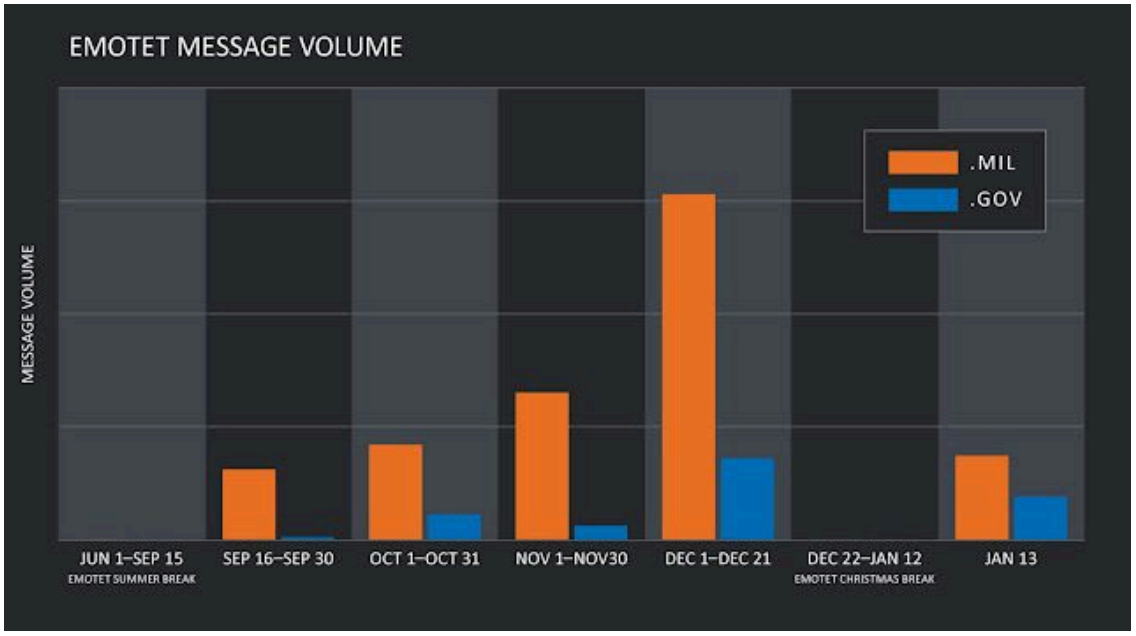
Cisco Talos continues to monitor Emotet, constantly detonating Emotet samples inside of the ThreatGrid malware sandbox and elsewhere. We witness in real-time as email that purports to be from Emotet's victims begins to emanate through Emotet's network of outbound mail servers. Vigilant monitoring of both stolen SMTP credentials and outbound email allows Talos to extract meta-information regarding Emotet's latest victims and provides insight into networks where Emotet is actively spreading.

One of the most cunning aspects of Emotet's propagation is the way they use social engineering of personal/professional relationships to facilitate further malware infection. When receiving a message from a trusted friend or colleague, it is quite natural for recipients to think, "I can safely open this email attachment because it is in reply to a message I sent, or from someone I know." Any person or organization who has sent an email to an Emotet victim could be targeted by Emotet's propagation messages. The more interaction with the victim you have, the more likely you are to receive malicious email from Emotet. Like a meandering watering hole attack, this is how Emotet crosses organizational boundaries with the potential to affect entire industries or even countries.

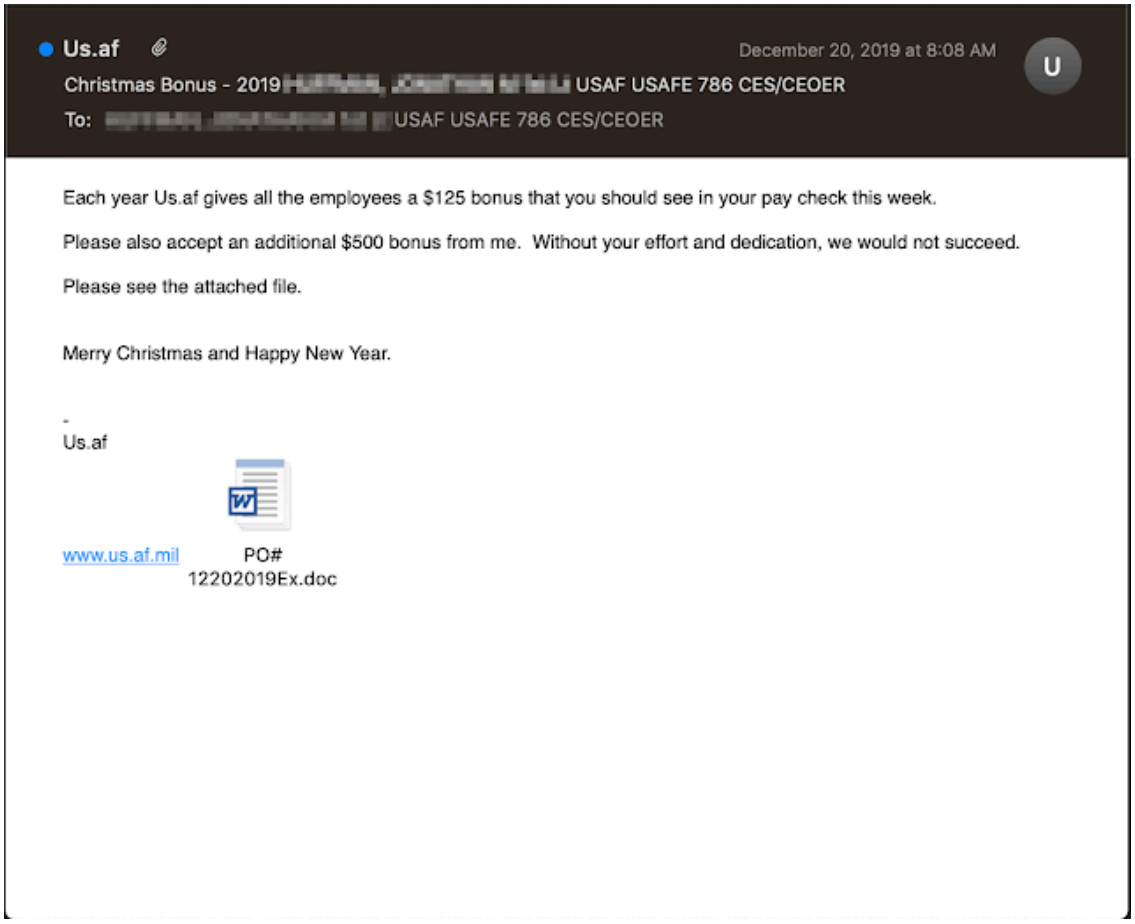
Increased targeting of U.S. military and government Emotet continues to infect individuals and organizations all over the world, so to say that it is "targeted" would be a stretch. However, if a person has substantial email ties to a particular organization, when they become infected with Emotet the effects would manifest in the form of increased outbound Emotet email directed at that organization.

One of the most vivid illustrations of this effect can be seen in Emotet's relationship to the .mil (U.S. military) and .gov (U.S./state government) top-level domains (TLDs). When Emotet emerged from its summer vacation back in mid-September 2019, relatively few outbound emails were seen directed at the .mil and .gov TLDs.

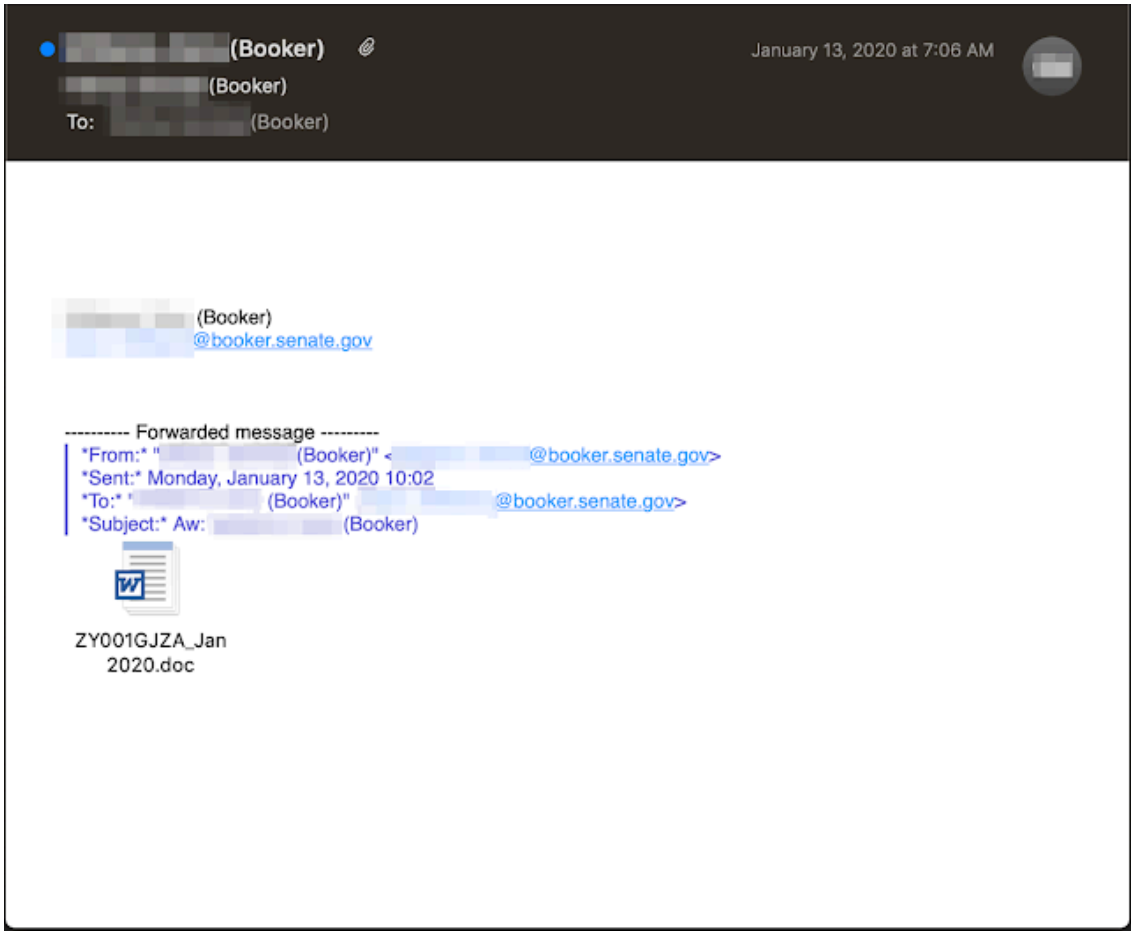
But sometime in the past few months, Emotet was able to successfully compromise one or more persons working for or with the U.S. government. As a result of this, Talos saw a rapid increase in the number of infectious Emotet messages directed at the .mil and .gov TLDs in December 2019. Now that Emotet is back from their Orthodox Christmas vacation, that trend has continued into January 2020.



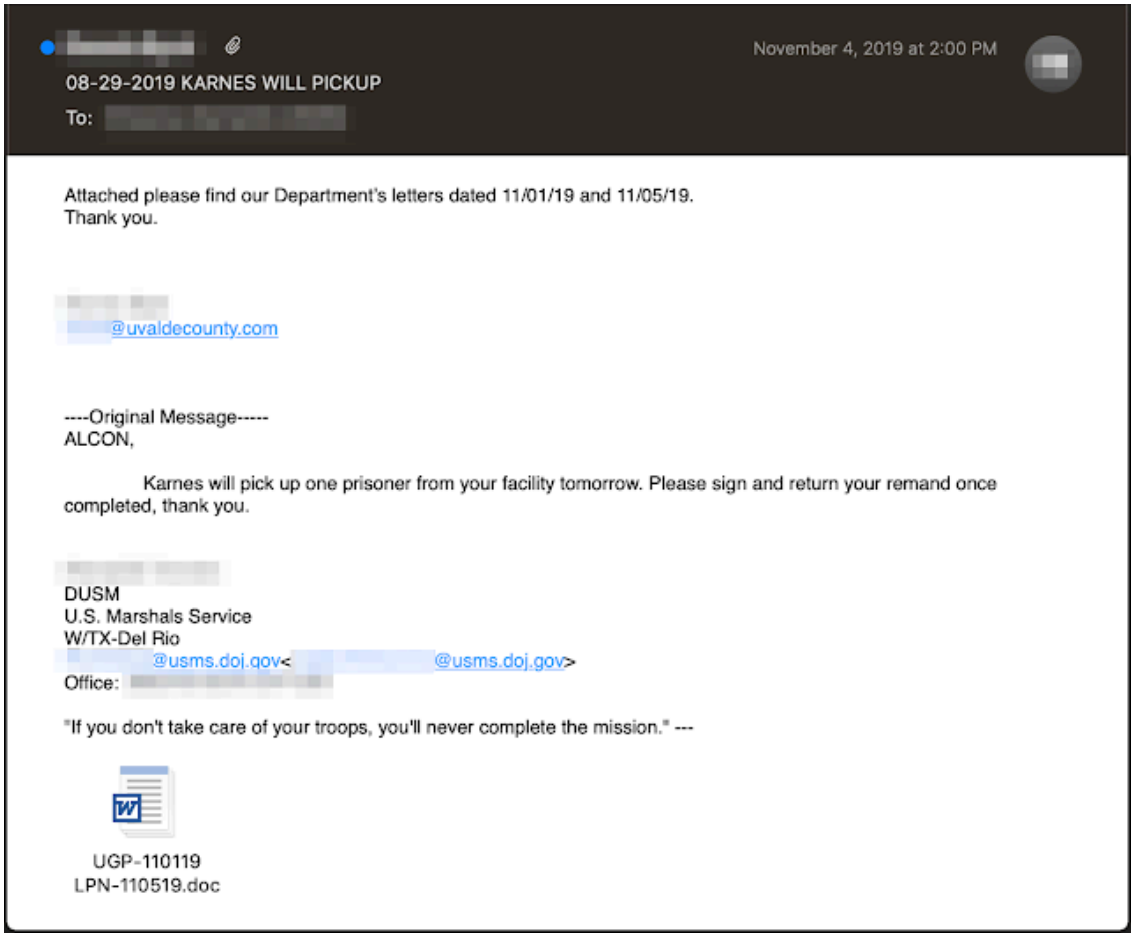
The emails are coming from inside the house! Looking at the individual messages sometimes allows us to determine the identity of the Emotet victim and whether that victim is internal or external to the recipient organization. After all, Emotet wants recipients of its messages to recognize who the message came from as part of their social engineering efforts. Unfortunately, this doesn't work 100 percent of the time, because some of the messages sent by Emotet strips the original victim's personal data and drops the TLD in an attempt to impersonate only the organization. This results in the unintentionally comical reduction of domains like "us.af.mil" to simply "Us.af."



However, more often, Emotet will leave the contact information for the individual victim inside the propagation email. The message may also include the contents of a previous email exchange between the two recipients, just to add extra authenticity. For example, the following message was sent by Emotet to an individual working for U.S. Sen. Cory Booker. The From header and signature generated by Emotet both suggest that this message originated from an infected colleague at "booker.senate.gov."



Another issue that is often overlooked is the exfiltration problem presented by Emotet. Users who have their email stolen and sent to Emotet's command and control (C2) infrastructure may have lost control over sensitive data and communications. For now, Emotet is content using this data to enhance its social engineering approach, but they could just as easily be reading/parsing the contents of these messages and acting/trading on the information contained therein.



Conclusion If an organization in close proximity to yours becomes infected with Emotet, you can expect to receive an increased volume of infectious email messages addressed to your users. If Emotet infects any of the users inside your domain, then the volume of Emotet email destined for your network will increase. Many of these email messages arrive via hijacked email threads, so there is no simple pattern that anti-spam systems can use to identify and eliminate these messages. More advanced anti-spam systems, such as IPAS, will still be able to successfully filter Emotet messages. However, all technical systems no matter how robust must always be supplemented by educational efforts and awareness training for your users.

Coverage Additional ways our customers can detect and block this threat are listed below.

Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Stealthwatch	N/A
Stealthwatch Cloud	N/A
Threat Grid	✓
Umbrella	✓
WSA	✓

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), andMeraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.
