Kronos Banking Trojan Used to Deliver New Point-of-Sale Malware

proofpoint.com/us/threat-insight/post/kronos-banking-trojan-used-to-deliver-new-point-of-sale-malware

November 15, 2016

November 15, 2016 Proofpoint Staff

Overview

Banking Trojans continue to evolve and threat actors are using them in new ways, even as the massive Dridex campaigns of 2015 have given way to ransomware and other payloads. Most recently, we observed several relatively large email campaigns distributing the Kronos banking Trojan. In these campaigns, though, Kronos acted as a loader with a new Point-of-Sale (POS) malware dubbed ScanPOS as the secondary payload.

These campaigns not only represent an uptick in our observed instances of Kronos banker but also a new application of the malware that was first introduced in June 2014 and that we most recently described in relation to campaigns targeting Canada [1].

Email Campaigns

On November 10 and 14, Proofpoint observed several large email campaigns of tens of thousands of messages each, targeting a range of verticals including hospitality, higher education, financial Services, and healthcare. The relative volumes by vertical are shown in Figure 1.

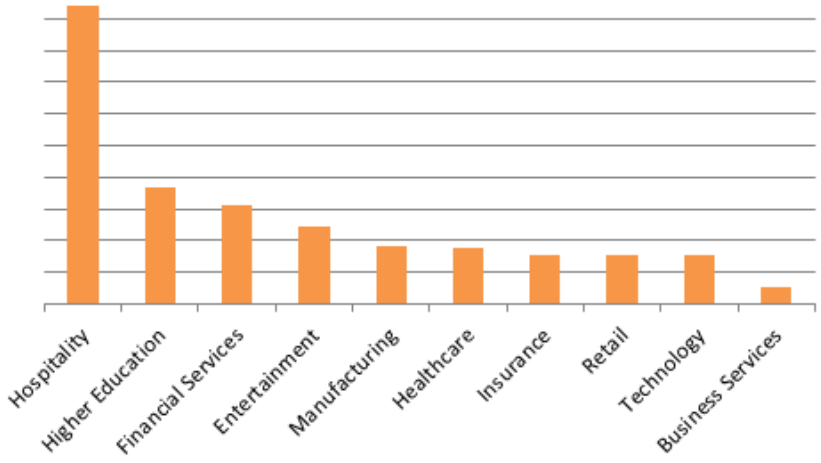


Figure 1: Vertical targeting across several campaigns

These campaigns reached global audiences but primarily targeted the United Kingdom and North America.

The email messages contained a document attachment or a link such as *hxxp://intranet.excelsharepoint[.]com/profile/Employee[.]php?id=[base64 encoded e-mail address]*. This domain is under attacker control but pretends to be associated with Microsoft SharePoint. Clicking the link causes the targeted user to download a malicious document (Fig. 2 and 3).

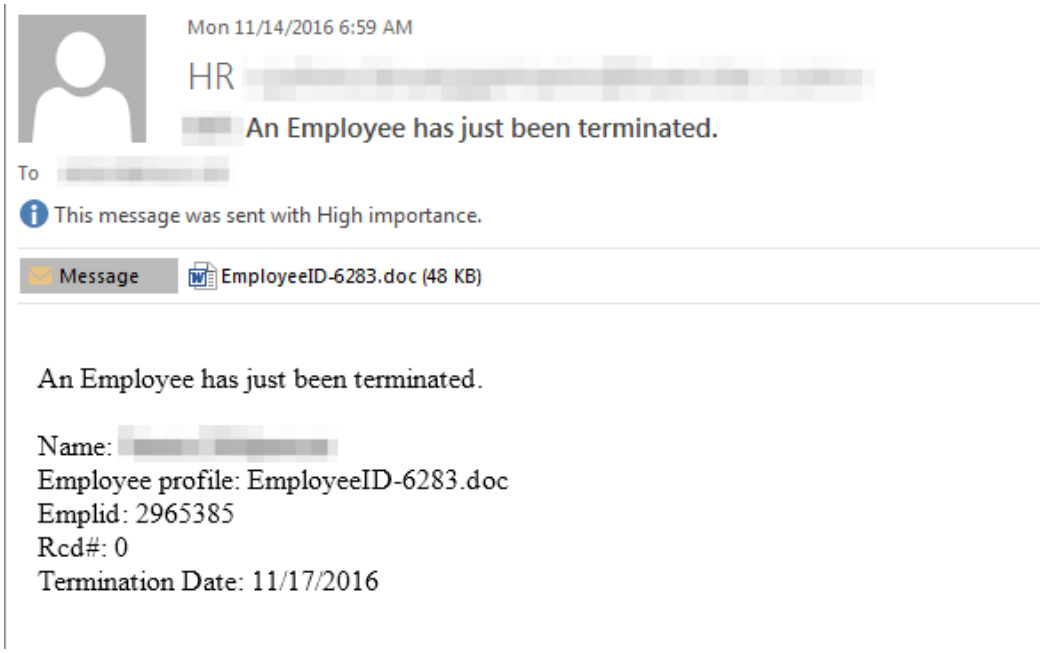
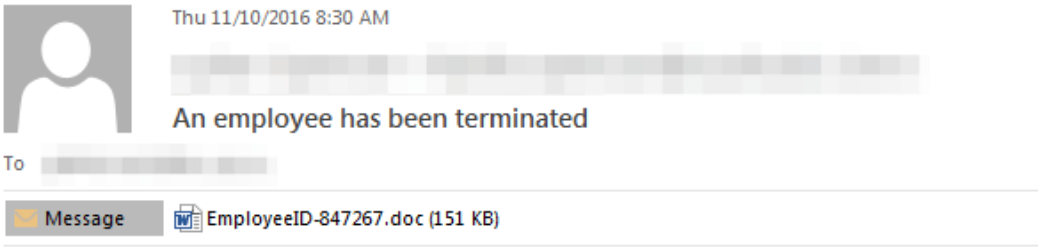


Figure 2: E-mail containing malicious attachment only



An Employee has just been terminated.

Name:

Employee profile: Link

Emplid: 847267

Rcd#: 0

Termination Date: 11/04/2016

=

Figure 3: Email containing malicious attachment and link to malicious document

The documents we observed contained a macro which downloaded Kronos [2] from a URL such as *hxxp://info.docs-sharepoint[.]com/officeup[.]exe* . The Kronos payload had a command and control (C&C) of *hxxp://www.networkupdate[.]club/kbps/connect[.]php* . The Kronos payloads received tasks to download at least three different payloads from the following URLs:

- *hxxp://networkupdate[.]online/kbps/upload/c1c06f7d[.]exe* - Smoke Loader
- *hxxp://networkupdate[.]online/kbps/upload/1f80ff71[.]exe* - Smoke Loader
- *hxxp://networkupdate[.]online/kbps/upload/a8b05325[.]exe* - ScanPOS

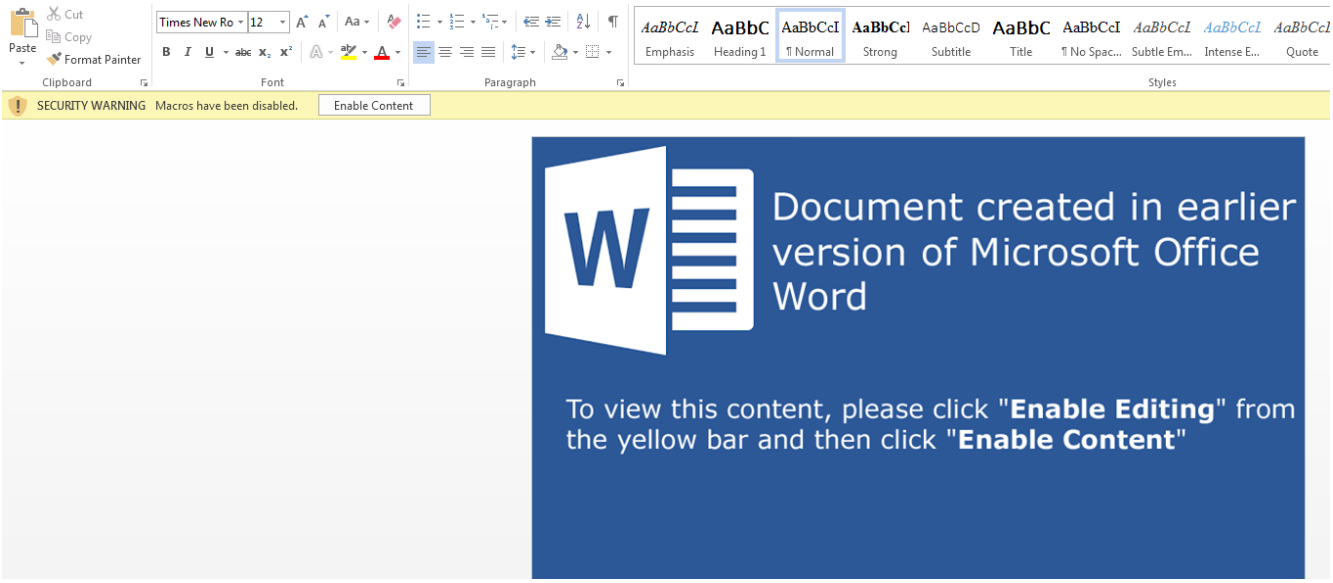


Figure 4: Malicious macro document with "Enable Content" lure

Both Smoke Loader [3] payloads were configured to use *hxxp://webfeed.updatesnetwork[.]com/feedweb/feed[.]php* as their C&C. So far we have not observed any additional payloads associated with these two Smoke Loader samples. However, as noted in the next section, we have observed a ZeuS variant payload being downloaded by a different Smoke Loader sample using the same C&C.

The third payload we observed is a new Point-of-Sale (POS) malware called ScanPOS that is capable of exfiltrating via HTTP (Fig. 5) credit card numbers that are discovered by searching in the memory of running processes. This new POS variant only has a single, hard-coded C&C: *hxxp://invoicesharepoint[.]com/gateway[.]php*. As with several other domains described here, these pretend to be associated with Microsoft SharePoint but are independent and under attacker control.

Exfiltrated data is base64 encoded and include:

- The stolen track data
- The process in which the data was found
- The username

Please refer to the discovery article by our colleagues at Morphick for additional technical analysis on this new POS variant [4].

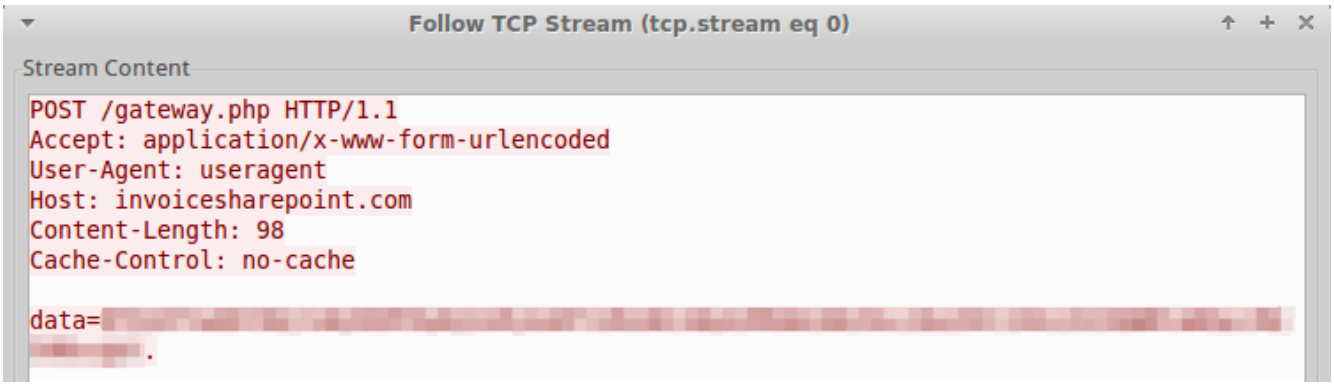


Figure 5: ScanPOS exfiltrating CC data over HTTP

Other Activity

In a November 8 campaign that preceded this activity, we observed similar emails and URLs following the same pattern as those used to deliver Kronos. However, in this campaign we observed links leading to RIG-v Exploit Kit (EK), followed by a redirect to ZIP-compressed .pif Smoke Loader and ZeuS. The links followed a pattern that was very similar to the more recent campaigns: *hxxp://invoice.docs-sharepoint[.]com/profile/profile[.]php?id=[base64 e-mail address]*. These links utilized an iframe to redirect potential victims to a RIG-v instance located at *add.souloventure[.]org* as well as to /download.php on the same server as the original link (Fig. 6).

Figure 6: Iframe redirect to RIG-v and payload download

Unfortunately, we did not observe any payloads delivered through this particular redirect chain. The /download.php returns an EmployeeID-47267.zip payload that we observed containing either a Smoke Loader variant using *hxxp://webfeed.updatesnetwork[.]com/feedweb/feed[.]php* as its C&C or a ZeuS variant using *hxxps://feed.networksupdates[.]com/feed/webfeed[.]xml* as its C&C. In the instance where we observed Smoke Loader, Smoke Loader downloaded an identical (same hash) ZeuS variant.

Conclusion

The campaigns distributing ScanPOS are heavily targeted at the hospitality vertical in North America and the UK, among other countries that observe the Christmas and/or Thanksgiving holidays. With the holidays approaching and their associated heavy travel and shopping, organizations should be especially vigilant with respect to potential infection with POS malware, banking Trojans, and other malware that may be used to exploit seasonal trends. We will continue to monitor Kronos campaigns, ScanPOS distribution, and other threats as they emerge.

References

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
hxxp://invoice.docs-sharepoint[.]com/profile/profile[.]php?id=[base64 e-mail address]	URL	Phishing link on Nov 8
hxxp://invoice.docs-sharepoint[.]com/profile/download[.]php	URL	Redirect from phishing link on Nov 8
4b5f4dbd93100bb7b87920f2f3066782a8449eb9e236efc02afe570c1ce70cf5	SHA256	EmployeeID-47267.zip containing SmokeLoader from /download.php on Nov 8

IOC	IOC Type	Description
90063c40cb94277f39ca1b3818b36b4fa41b3a3091d42dfc21586ad1c461daa0	SHA256	SmokeLoader EmployeeID-47267.pif
711431204071b1e6f5b5644e0f0b23464c6ef5c254d7a40c4e6fe7c8782cd55c	SHA256	EmployeeID-47267.zip containing ZeuS from /download.php on Nov 8
4ba3913d945a16c099f5796fdeef2fda5c6c2e60cb53d46a1bfae82808075d74	SHA256	ZeuS EmployeeID-47267.pif
hxxps://feed.networksupdates[.]com/feed/webfeed.xml	URL	ZeuS C&C on Nov 8
add.souloventure[.]org	Domain	RIG-v domain on Nov 8
hxxp://intranet.excelsharepoint[.]com/profile/Employee[.]php?id=[base64 e-mail address]	URL	Phishing link on Nov 10
a78b93a11ce649be3ca91812769f95a40de9d78e97a627366917c4fcd747f156	SHA256	EmployeeID-847267.doc downloaded from phishing links on Nov 10
hxxp://info.docs-sharepoint[.]com/officeup[.]exe	URL	EmployeeID-847267.doc downloading payload (Kronos) on Nov 10
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	SHA256	Kronos on Nov 10
hxxp://www.networkupdate[.]club/kbps/connect[.]php	URL	Kronos C&C on Nov 10
hxxp://networkupdate[.]online/kbps/upload/c1c06f7d[.]exe	URL	Payload DL by Kronos on Nov 10
hxxp://networkupdate[.]online/kbps/upload/1f80ff71[.]exe	URL	Payload DL by Kronos on Nov 10
hxxp://networkupdate[.]online/kbps/upload/a8b05325[.]exe	URL	Payload DL by Kronos on Nov 10

IOC	IOC Type	Description
d0caf097ea0350dc92277aed73b0f44986d7d85b06d1d17b424dc172ce35a984	SHA256	c1c06f7d.exe - SmokeLoader
d9d1f02c8c4beee49f81093ea8162ce6adf405640ccacd5f03ce6c45e700ee98	SHA256	1f80ff71.exe - SmokeLoader
hxxp://webfeed.updatesnetwork[.]com/feedweb/feed[.]php	URL	SmokeLoader C&C
093c81f0b234c2aa0363129fdaaaf57551f161915da3d23f43a792b5f3024c1e	SHA256	a8b05325.exe - ScanPOS
hxxp://invoicesharepoint[.]com/gateway[.]php	URL	ScanPOS C&C
hxxp://intranet.excel-sharepoint[.]com/doc/employee[.]php?id=[base64 e-mail address]	URL	Phishing link on Nov 14
fd5412a7c71958ecdffa7064bf03c5f1931e561a1e71bc939551d5afb8bf7462	SHA256	downloaded from phishing links on Nov 14
hxxp://profile.excel-sharepoint[.]com/doc/office[.]exe	URL	EmployeeID-6283.doc downloading payload (Kronos) on Nov 14
269f88cfa9e9e26f3761aedee5d0836b5b82f346128fe03da28a331f80a5fba3	SHA256	Kronos on Nov 14 (same C&C as previous)

ET and ETPRO Suricata/Snort Coverage

2018125	ET CURRENT_EVENTS SUSPICIOUS .PIF File Inside of Zip
2020077	ET TROJAN Kronos Checkin M2
2020080	ET TROJAN Kronos Checkin
2022124	ET TROJAN Win32.Sharik Microsoft Connectivity Check
2022550	ET CURRENT_EVENTS Possible Malicious Macro DL EXE Feb 2016
2023196	ET CURRENT_EVENTS RIG EK Landing Sep 12 2016 T2
2023401	ET CURRENT_EVENTS RIG EK URI struct Oct 24 2016 (RIG-v)
2816808	ETPRO CURRENT_EVENTS RIG EK Flash Exploit Mar 29 2016
2823254	ETPRO TROJAN ScanPOS Exfiltrating CC Data
2823288	ETPRO TROJAN Zeus Variant CnC SSL Cert

Subscribe to the Proofpoint Blog