Fake Jobs: Campaigns Delivering More_eggs Backdoor via Fake Job Offers

proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers

February 21, 2019

Blog
Threat Insight
Fake Jobs: Campaigns Delivering More_eggs Backdoor via Fake Job Offers

February 21, 2019 Proofpoint Threat Insight Team

Overview

Since the middle of 2018, Proofpoint has been tracking campaigns abusing legitimate messaging services, offering fake jobs, and repeatedly following up via email to ultimately deliver the More_eggs backdoor. These campaigns primarily targeted US companies in various industries including retail, entertainment, pharmacy, and others that commonly employ online payments, such as online shopping portals.

The actor sending these campaigns attempts to establish rapport with potential victims by abusing LinkedIn's direct messaging service. In direct follow-up emails, the actor pretends to be from a staffing company with an offer of employment. In many cases, the actor supports the campaigns with fake websites that impersonate legitimate staffing companies. These websites, however, host the malicious payloads. In other cases, the actor uses a range of malicious attachments to distribute More_eggs.

We also believe that the same actor recently sent related campaigns, first noted by Brian Krebs, targeting anti-money laundering officers at financial institutions [1].

Delivery

We have observed a number of variations among the campaigns, but most share common characteristics. While not exhaustive, the general flow as well as specific examples of these attacks are described below.

Initially the actor uses a fraudulent, but legitimately created LinkedIn profile to initiate contact with individuals at the targeted company by sending invitations with a short message (Figure 1). This appears as a benign email with the subject "Hi [Name], please add me to your professional network".

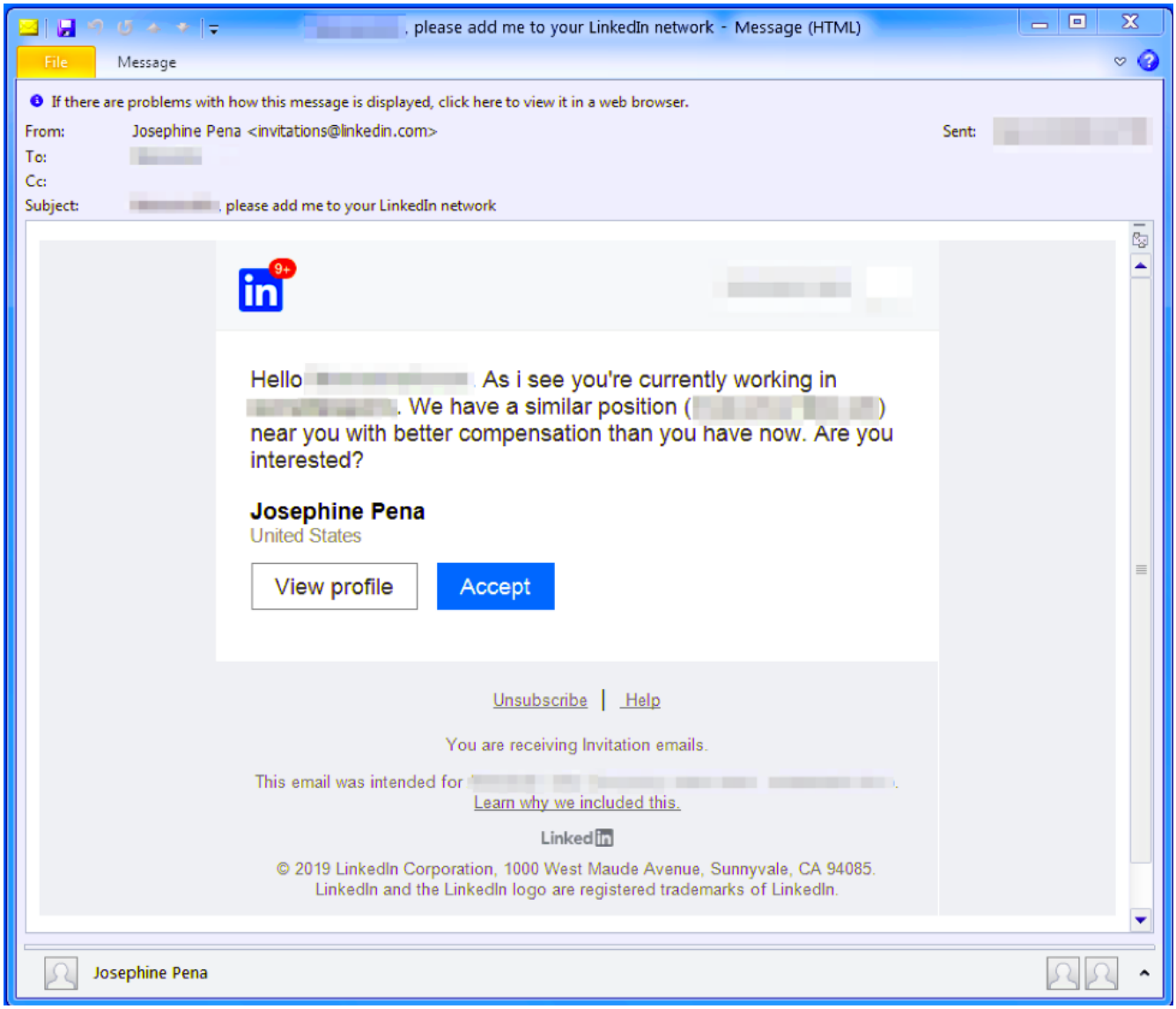

Figure 1: Example of initial message in which attackers abuse LinkedIn messaging.

Within a week, the actor sends a direct email to the target's work address reminding the recipient about the prior attempt to communicate on LinkedIn (Figure 2). It uses the target's professional title, as it appears on LinkedIn, as the subject, and often suggests the recipient click on a link to see the noted job description. In other cases, this actor used an attached PDF with embedded URLs or other malicious attachments.

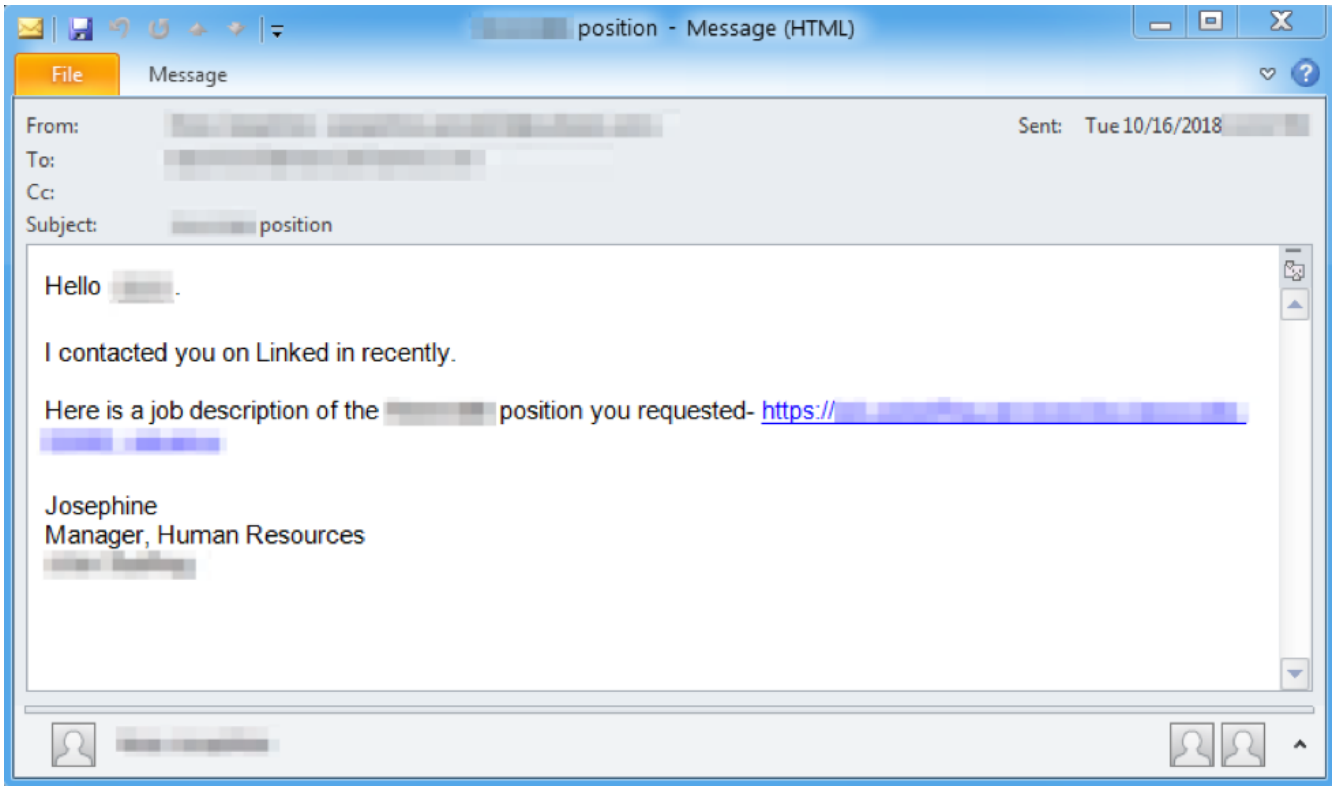

Figure 2: Example follow up email to the target's work address, with a malicious URL.

The URLs link to a landing page that spoofs a real talent and staffing management company, using stolen branding to enhance the legitimacy of the campaigns (Figure 3). The landing page initiates a download of a Microsoft Word file (Figure 4) with malicious macros created with Taurus Builder (described below). If the recipient enables macros, the "More_eggs" payload will be downloaded and executed. In other cases, the landing page may initiate the download of a JScript loader instead, but this intermediate malware still ultimately results in the delivery of More_eggs.

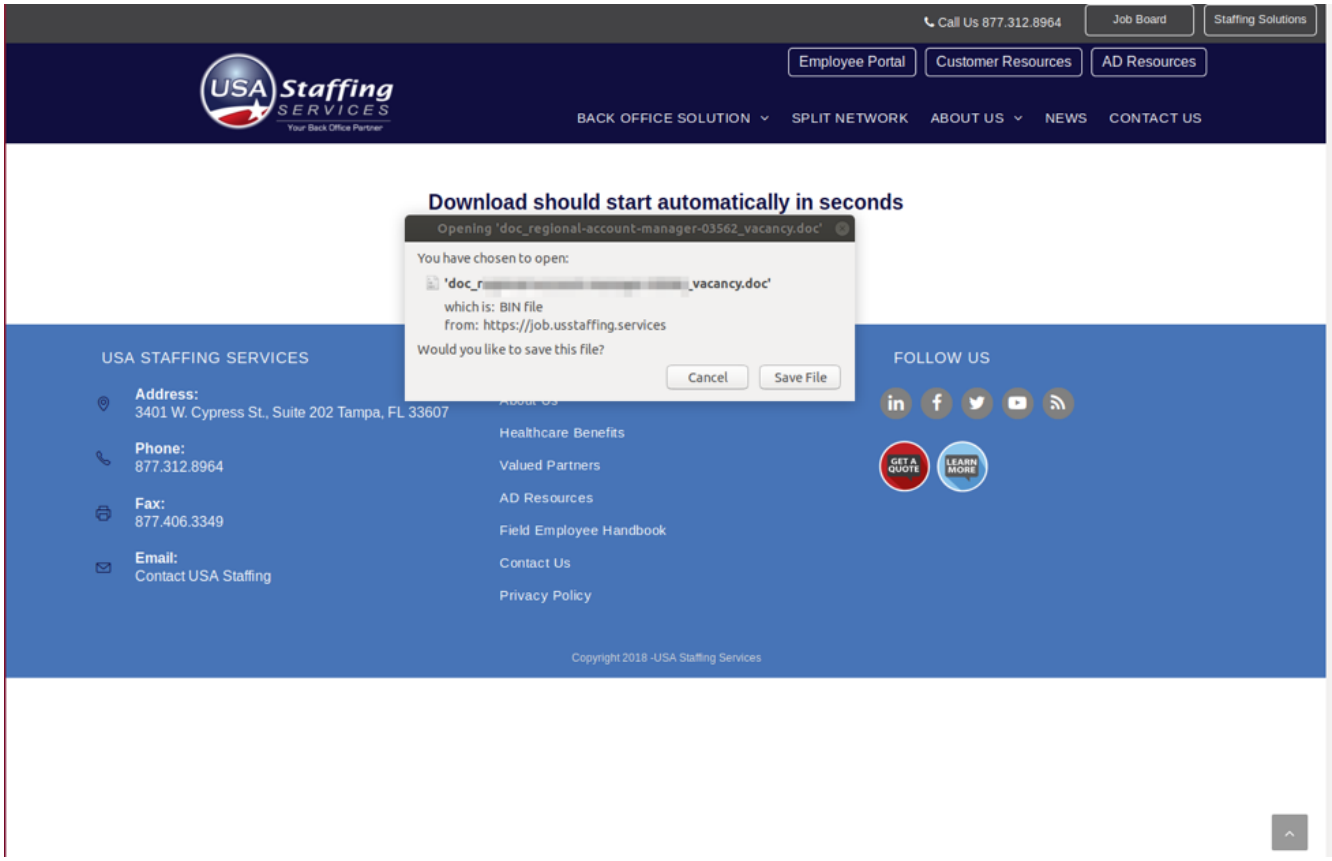

Figure 3: Example of a landing page for the URL included in email using stolen branding and a lookalike domain for a talent management agency. This one specifically initiates a download of a malicious Microsoft Word document.

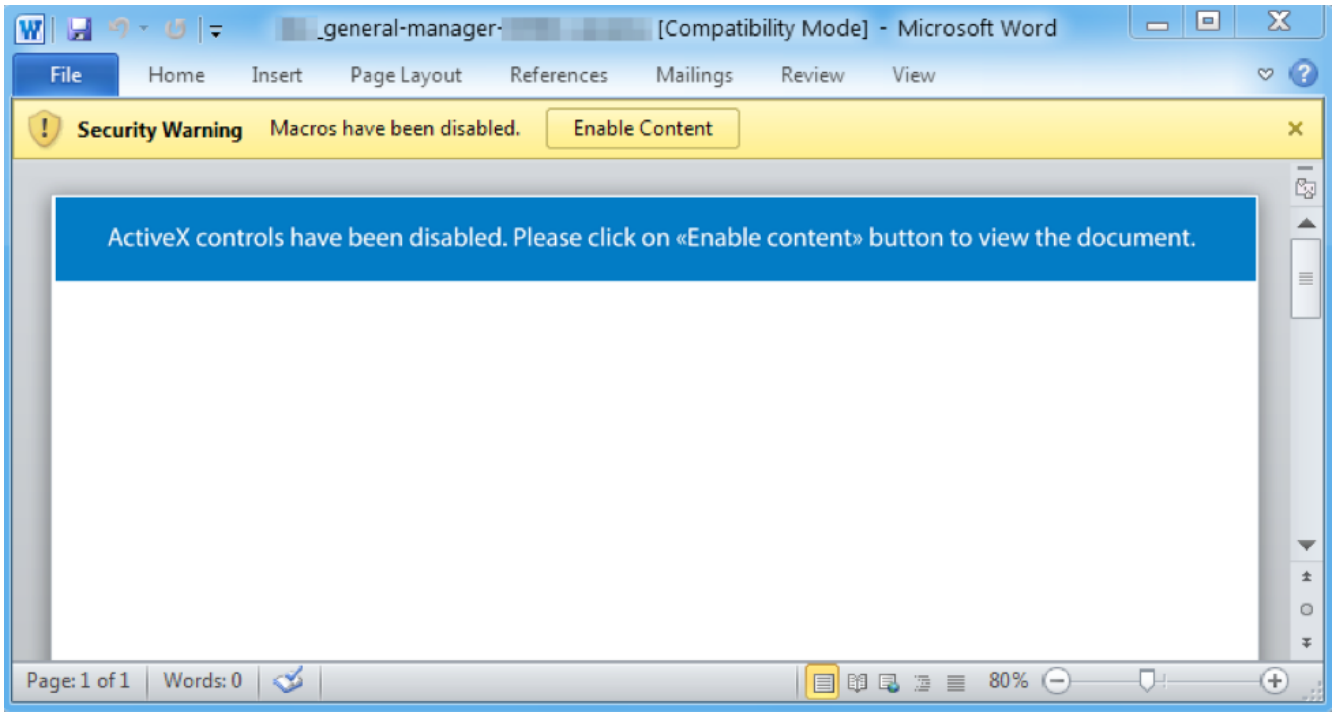

Figure 4: Example malicious Microsoft Word document that uses macros to download More_eggs.

As noted, some campaigns also used malicious attachments instead of URLs in the email. Figure 5 shows an example of one such attachment, a PDF with a link to a spoofed landing page like that shown in Figure 3.

Figure 5: Example PDF attachment that contains a malicious URL.

Variations

These campaigns demonstrated considerable variability, with the actor frequently changing delivery methods and more. Examples of the types of techniques used by the actor to deliver the final More_eggs payload include:

- URL linking to a landing page that initiates the download for an intermediate JScript loader or Microsoft Word document with macros or exploits
- URL shortener redirecting to the same landing page
- PDF attachment with a URL linking to the same landing page
- Password-protected Microsoft Word attachment with macros that download More_eggs
- Completely benign emails without a malicious attachment or URL attempting to further establish rapport (Figure 6)

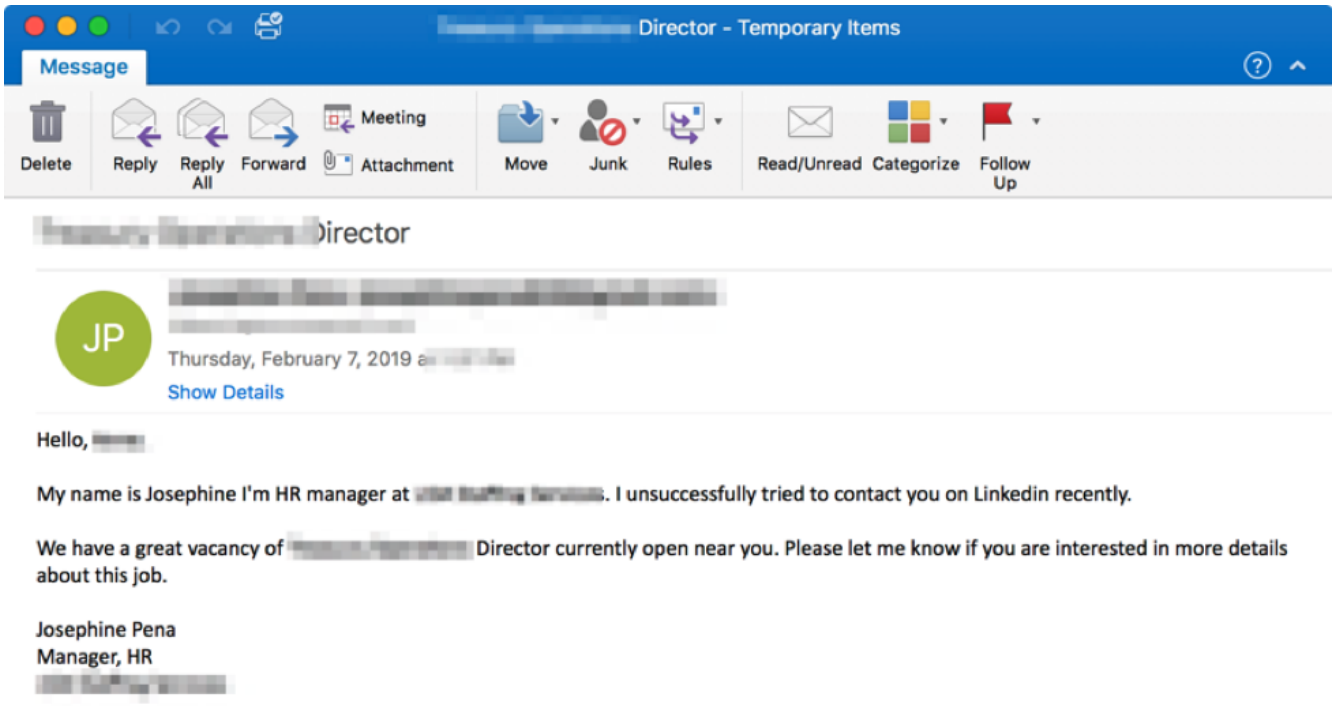

Figure 6: Example of a benign email designed to establish rapport with potential victims

Tools

This actor uses a variety of tools to distribute malware. We briefly describe three such tools below.

Taurus Builder

We use this name to describe a tool used to create malicious documents. We believe Taurus builder was purchased on underground crime forums. Notably, documents created with this builder use the CMSTP bypass as described in [2]. Both Palo Alto Networks [3] and QuoScient [4] have previously described documents created with this kit.

VenomKit

We use this name to describe documents generated by a builder purchased from the same seller as Taurus builder. Depending on the variant it may exploit CVE-2017-0199, CVE-2017-8570, CVE-2017-8759, CVE-2017-11882, CVE-2018-0802, and/or CVE-2018-8174. Notably, VenomKit often also uses the same CMSTP bypass as Taurus. Documents from this kit have previously been discussed by Quoscient [4].

More_eggs

More_eggs is malware written in JScript used in these campaigns and others. It is often used as a downloader. In addition to its ability to download additional payloads, More_eggs has extensive capabilities to profile the infected machine. The malware was first documented by Trend Micro [5].

Overlaps with Anti-Money Laundering Campaign

Brian Krebs wrote about a related campaign that targeted anti-money laundering officers at financial institutions that we believe may have been sent by the same actor. Although targeting and the final payload were different in the campaign he described, key similarities to campaigns describe above included:

- The use of a similar PDF email attachment to the PDFs used in the Fake Jobs campaigns
- The PDFs of both the anti-money laundering campaign and the Fake Jobs campaigns at one point included URLs hosted on the same domain

Large Follow-up Spam Campaign

Note: As we were finalizing this report we observed a larger than usual campaign from this actor on Feb 21, 2019, from random senders, with a malicious URL in the email.

Conclusion

As threat actors continue to turn away from very large-scale “spray and pray” campaigns and focus on persistent infections with downloaders, RATs, bankers, and other malware, increasingly sophisticated social engineering and stealthy malware are making their way into a range of campaigns. This actor provides compelling examples of these new approaches, using LinkedIn scraping, multi-vector and multistep contacts with recipients, personalized lures, and varied attack techniques to distribute the More_eggs downloader, which in turn can distribute the malware of their choice based on system profiles transmitted to the threat actor. In response to the increasing effectiveness of layered defenses and end user education efforts, we can expect more threat actors to adopt approaches that improve the effectiveness of their lures and increase the likelihood of high-quality infections.

Note: We have informed all affected parties about the abuse of their services and brands in these campaigns.

References

[1]https://krebsonsecurity.com/2019/02/phishers-target-anti-money-laundering-officers-at-u-s-credit-unions/

[2]https://bohops.com/2018/02/26/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence/

[3]https://unit42.paloaltonetworks.com/unit42-new-techniques-uncover-attribute-cobalt-gang-commodity-builders-infrastructure-revealed/

[4]https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

[5]https://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-carrying-emails-set-sights-on-russian-speaking-businesses/

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
interrafcu[.]com	Domain	Landing Page Domain
usstaffing[.]services	Domain	Landing Page Domain
edb39c4eb28cf526f1e606365cdef009cb9aa8ba99feb448db615326bf495042	SHA256	Example Taurus Builder Document
hxxp://204.155.30[.]109/3521.txt	URL	Document Payload
d39cb07e97fd91e75c51f75ccef1a8d7ce8ec8c951943501f981ce98d6319e01	SHA256	Scriptlet leading to More_eggs
2bca33c8be6483aec5cbb29d18c5f626a86205fca92191468b8b1032d38aebea	SHA256	Example VenomKit Document
2470ac1632546ecf5c9c9d93c6dc088253ba682ba9cf19ae6984b6cee3f8e2b5	SHA256	Example Code Signed JS Loader
73defd8066549e5b09c509064bc5bd29e77eca2c18d114c0bcf3dfa1cefe6939	SHA256	Example JS Loader
mail[.]rediffmail[.]kz	HostName	More_Eggs C&C
onlinemail[.]kz	HostName	More_Eggs C&C
api[.]cloudservers[.]kz	HostName	More_Eggs C&C
secure[.]cloudserv[.]ink	HostName	More_Eggs C&C

tonsandmillions[.]com	HostName	More_Eggs C&C
contactlistsagregator[.]com	HostName	More_Eggs C&C

ET and ETPRO Suricata/Snort Signatures

2832245 | ETPRO CURRENT_EVENTS Possible More_eggs Connectivity Check

2834137 | ETPRO TROJAN Observed Malicious SSL Cert (More_eggs CnC)

Subscribe to the Proofpoint Blog