Deloitte.

The evolution of the Nymaim Criminal Enterprise

Threat Intelligence & Analytics

Threat Study

Issue Date: September 14, 2016 | TLP: White | Serial: W-TS-EN-16-00758 | Industry: All

Contents

Prologue

Financially motivated threat actors often operate in ways similar to those of legitimate businesses, despite the illegal nature of their actions. As with legitimate businesses, some criminal operations are more customer-centric than others. Threat actors that collect payment card information (PCI), online banking credentials, personally identifiable information (PII), or protected health information (PHI) usually sell that data to criminal customers on underground markets, who use it for fraud. Consumers of such data often seek data from specific geographic areas or financial institutions, so as to facilitate its monetization through whatever fraud infrastructure they may have, such as a network of mules to cash out bank accounts, receive fraudulently purchased packages, or use fraudulent copies of credit cards for in-store purchases.

The monetization of ransomware infections is simpler than that of compromised banking credentials, PCI, PII, or PHI. Ransomware actors collect payments directly from their victims, rather than selling their victims' data to third parties. Ransomware operations thus do not have customers per se, although the ransom notes of some ransomware families may address their victims as if they were the customers of a legitimate business, in the hopes of persuading victims to pay. The simpler monetization of ransomware may have contributed to the escalating number of ransomware attacks and proliferation of new ransomware families in the first half of 2016.

At least one criminal group has defied this overwhelming trend in favor of ransomware – the one responsible for the Nymaim malware downloader and its GozNym banking Trojan variant. This group shifted from its previous use of ransomware against victims for nearly two years and has instead begun to target their online banking credentials. There is no indication of why this group would undertake this shift after using ransomware for so long and go against the leading trend in criminal malware in order to conduct a type of attack whose monetization is more complex. It is possible that the group concluded that the ransomware market was saturated and thus decided to move into online banking attacks instead, but this shift began in November 2015 – before the current spike in ransomware attacks and proliferation of new ransomware families began.

Another possibility is that the obsolescence of this group's historic police ransomware payloads left it less capable of competing with the newer and more sophisticated crypto-ransomware families. Police ransomware locks a victim's screen and uses a law enforcement-themed message to demand a "fine" for allegedly illegal online activities. This form of ransomware has declined, as crypto-ransomware, which encrypts a victim's files and holds them for ransom, has now become the prevailing form of ransomware. This point nonetheless raises the question of why the group did not simply begin to use a newer, more advanced crypto-ransomware payload instead.

Like legitimate businesses, criminal threat actors may have criminal vendors from whom they purchase products and services that they need for their own operations. Like many legitimate technology providers, they may also complement any proprietary or third-party products or services with openly available code. In the case of criminal actors, this freely available code may come from leaks or the recycling of source code for criminal malware families on underground threat actor forums. In the case of the Nymaim group, they may have originally recycled their historic ransomware payload from that of another group. The Nymaim group also reused existing banking Trojan code when it shifted to online banking attacks as well. Indeed, it is possible that the Nymaim downloader, the core of this group's operations, may be its only original contribution to those operations. In any event, it has made that downloader the centerpiece of an enterprise that otherwise relies extensively on products, services, and code from other actors.

Executive Summary

The Nymaim malware family, which includes its original downloader and its newer GozNym banking Trojan variant, has been active since at least 2013. Its origins are unclear, and it may be the proprietary product of a criminal actor or group that developed it and retains exclusive access to it. Some trends in the use of Nymaim and its variants over the past three years lend additional credence to that possibility. If Nymaim activity is the product of just one group, that group has nonetheless relied extensively on a variety of external services and sources for both initial infection vectors and second-stage malware payloads.

Nymaim's infection vectors have shifted repeatedly over the course of three years. A recurring theme in many of those infection vectors has been the involvement of other threat actors and groups that may have provided these infection-enabling services to Nymaim operators. These other actors have included TA530, Dmitry "Paunch" Fedotov, and the operators of the botnet that spreads the Dridex banking Trojan and Locky ransomware. Despite these shifts in infection vectors, lure documents that mimic the branding of accounting software vendors have been a recurring theme in Nymaim-related attacks since 2015.

Police ransomware was Nymaim's typical second-stage payload from its emergence in 2013 until 2015. Nymaim operators may have recycled elements of previous Romanian ransomware into their own ransomware payloads. Nymaim shifted toward the compromise of online banking credentials. This shift culminated in the April 2016 emergence of GozNym, which combined elements of both Nymaim and the Gozi ISFB banking Trojan, AKA Ursnif.[1]

Nymaim's early ransomware payloads targeted a wide range of countries. Its geographic focus narrowed as it shifted toward online banking attacks. Key areas of interest include English-speaking North America, German-speaking Central Europe, Poland, Portugal and Brazil.[2]

Origins and Ownership

The source and origins of the Nymaim downloader remain an intelligence gap for the security community nearly three years after Nymaim's emergence. There is no specific information on who developed Nymaim and who has been deploying it in the wild. As of this writing, there is no significant evidence that it is available to the criminal actor community on underground forums, either for sale or via leaks of its source code.

This ostensible unavailability to the general criminal community raises the likely possibility that the unidentified developers of Nymaim have retained exclusive use of and access to it as their own proprietary downloader.[3] Although the infection vectors and payloads of Nymaim-related attacks have shifted over time, other factors would be consistent with the coordinated operations of a single group. These factors include: the degree of consistency in Nymaim-related attacks; the recurring accounting software theme in their lure documents; and their clearer geographic focus since the 2015 shift to online banking targets.

Shifting Infection Vectors

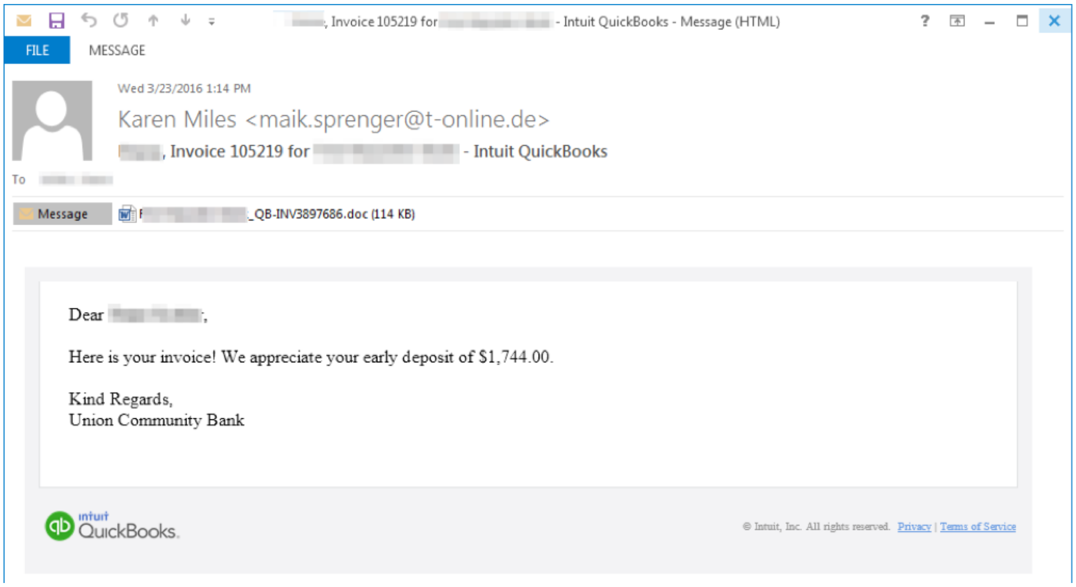
Nymaim first surfaced in July 2013 as one of many payloads that the "Home Campaign" of a specific instance of the Black Hole Exploit Kit (BHEK) delivered.[4] The arrest of BHEK operator Dmitry "Paunch" Fedotov may have prompted Nymaim to switch its infection vector to blackhat search engine optimization (SEO) in fall 2013. This application of SEO techniques raised the Google search engine ranking of links that redirected victims to archives that contained malicious executables with file names relevant to the targeted search terms. Users may have been more likely to open these files because they had been searching for such information.[5] Blackhat SEO services are widely available on underground forums.

Spam had become another infection vector for Nymaim by December 2015, when Nymaim samples surfaced in a spam run from the botnet that distributes both the Dridex banking Trojan and Locky ransomware.[6] By February 2016, however, Nymaim operators had begun using a novel infection vector: legitimate bulk email marketing services, which may have enabled this campaign to bypass spam filters. These email messages contained malicious attachments or links to malicious documents that used malicious macros to infect victims. It is unclear if the group used compromised accounts for such services or gained access to them via legitimate means.[7]

As of Q1 2016, Nymaim had also begun to appear as one of several different payloads in spear-phishing attacks by TA530, a provider of spear-phishing services to other actors. The distinctive feature of TA530 campaigns is the customization of spear-phishing email messages to individual targets on an unusually large scale, such as the use of correct names and contact and employment information for hundreds of thousands of targets. Those TA530 spear-phishing attacks that delivered Nymaim payloads used documents with malicious macros. These Nymaim attacks may have specifically aimed to infect the computers of employees who might conduct online banking sessions on behalf of their companies, which Nymaim operators could compromise with web injection attacks after delivering Gozi ISFB as a second-stage payload.[8] TA530 continued to use malicious macros to deliver Nymaim payloads to North American targets as of late May 2016.[9]

The only Nymaim infection vector to persist from 2013 to 2016 is the deployment of Nymaim as a second-stage payload via the separate Pony loader, AKA Fareit.[10]The Pony loader is available in underground threat actor communities, both for sale and through leaks of its source code.[11]

Another recurring theme in Nymaim attacks has persisted in their lure documents since the 2015 shift to banking attacks, despite shifts in infection vectors. This recurring theme further suggests that these Nymaim attacks may have specifically aimed to compromise the computers of employees with access to corporate bank accounts. These attacks have often disguised their malicious documents or links as either invoices or other transaction documents generated by Intuit accounting software, such as Quicken or Quickbooks, or as updates for such Intuit software packages.[12] In April 2016, some Nymaim samples also began to mimic the branding of Freshbooks, a different brand of accounting software, in similar lure documents.[13]



[redacted], Invoice 105219 for [redacted] - Intuit QuickBooks - Message (HTML)

Wed 3/23/2016 1:14 PM

Karen Miles <maik.sprenger@t-online.de>

[redacted], Invoice 105219 for [redacted] - Intuit QuickBooks

To [redacted]

F[redacted]_QB-INV3897686.doc (114 KB)

Dear [redacted],

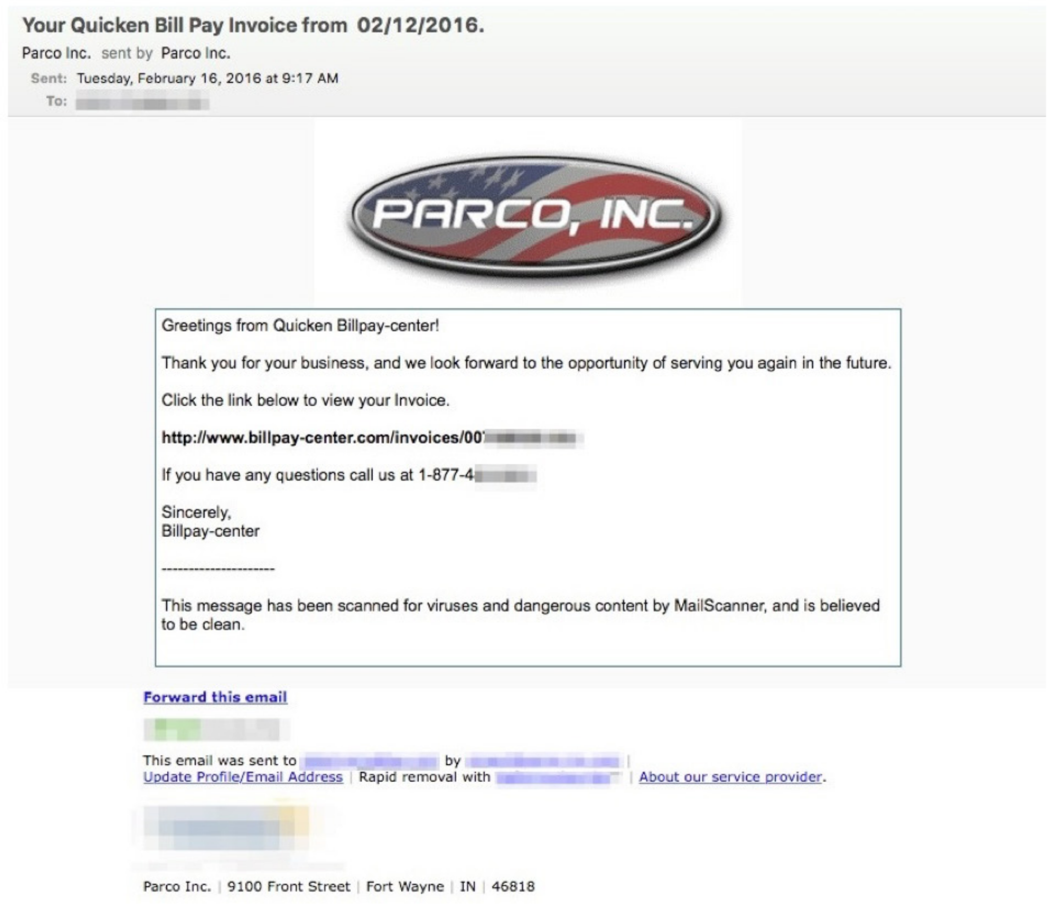
Here is your invoice! We appreciate your early deposit of $1,744.00.

Kind Regards,
Union Community Bank

© Intuit, Inc. All rights reserved. Privacy | Terms of Service

Figure 1: TA530 Nymaim attack email message [14]

Invoices are a typical financial theme for malicious documents or links in criminal spam or phishing attacks in general. It is also common for threat actors to disguise malicious files or links as updates for popular software, such as Adobe Flash Player. Nonetheless, this repeated mimicking of the branding of specific accounting software packages in social engineering lures, for both financially-themed attacks and fake software updates, is uncommon.[15]



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]

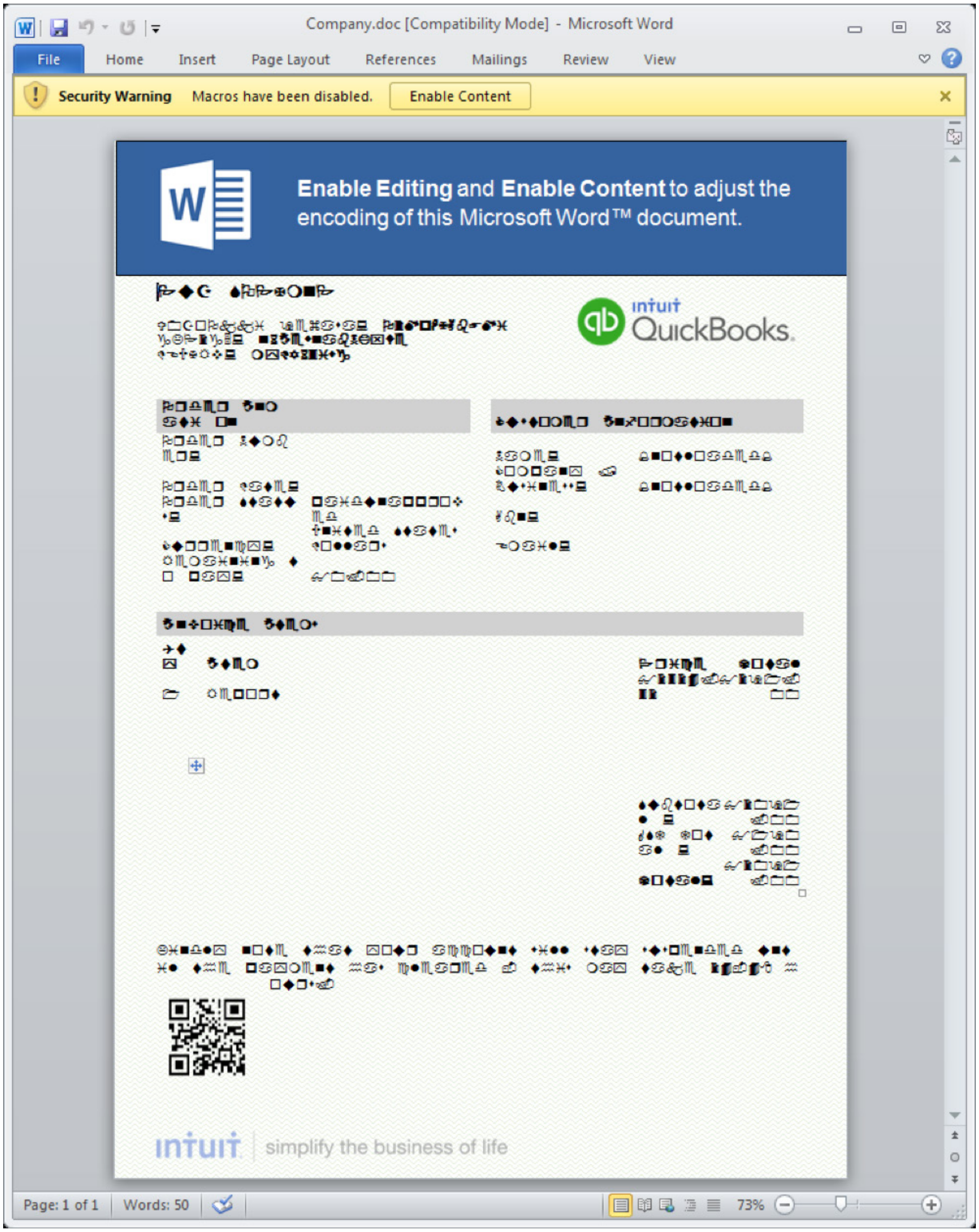
This email was sent to [redacted] by [redacted] |
Update Profile/Email Address | Rapid removal with [redacted] | About our service provider.

[redacted]

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

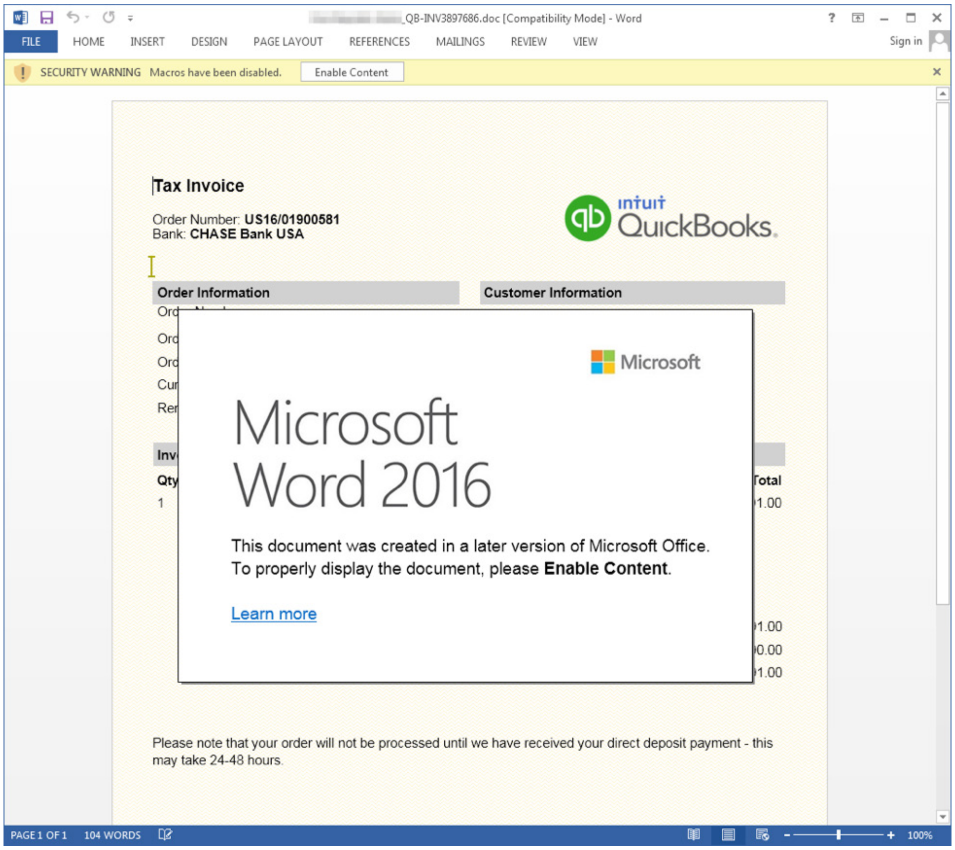
Figure 2: Nymaim attack email message from legitimate marketing service[16]

The use of such social engineering content would be consistent with the targeting of corporate bank accounts. The branding of such accounting software may be familiar to employees who have access to corporate bank accounts, such as those in Accounts Payable or Accounts Receivable. Such employees may thus be more likely to fall for this social engineering and click on the malicious link or document out of force of habit. Other employees would be less likely to recognize the branding of this accounting software or associate it with their official responsibilities, and their computers would be of less value to banking Trojan actors, given the lower likelihood of compromising online banking credentials on those computers.



Enable Editing and **Enable Content** to adjust the encoding of this Microsoft Word™ document.

Figure 3: TA530 malicious macro document that delivered Nymaim[17]



[redacted]_QB-INV3897686.doc [Compatibility Mode] - Word

SECURITY WARNING Macros have been disabled. Enable Content

Tax Invoice

Order Number: **US16/01900581**
Bank: **CHASE Bank USA**

intuit QuickBooks.

Order Information

Customer Information

Microsoft

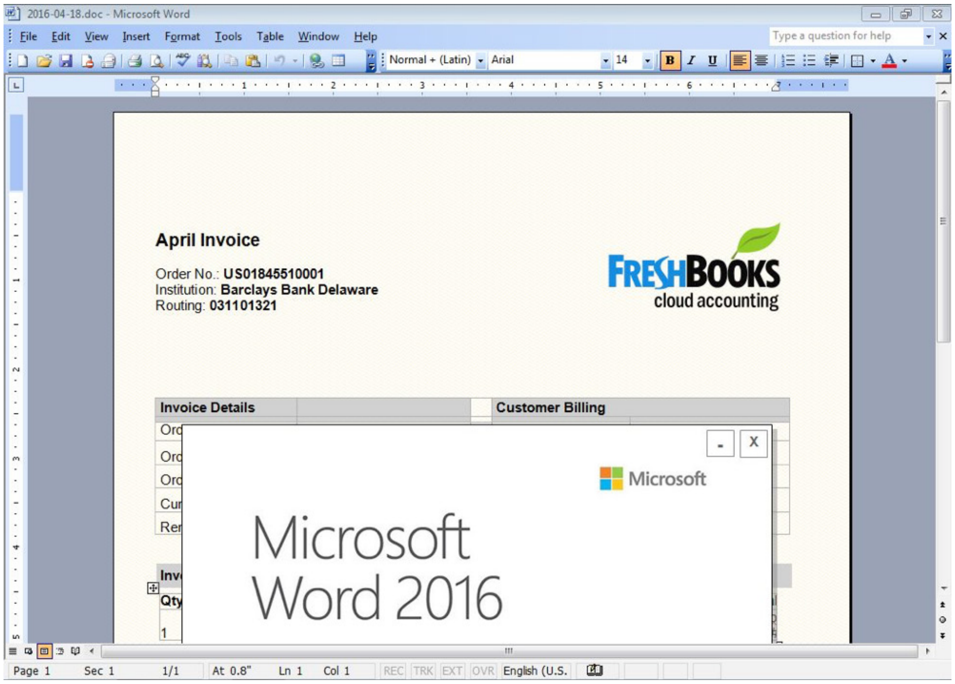
Microsoft
Word 2016

This document was created in a later version of Microsoft Office.
To properly display the document, please **Enable Content**.

Learn more

Please note that your order will not be processed until we have received your direct deposit payment - this may take 24-48 hours.

Figure 4: TA530 malicious macro document that delivered Nymaim[18]



2016-04-18.doc - Microsoft Word

April Invoice

Order No.: **US01845510001**
Institution: **Barclays Bank Delaware**
Routing: **031101321**

FRESHBOOKS cloud accounting

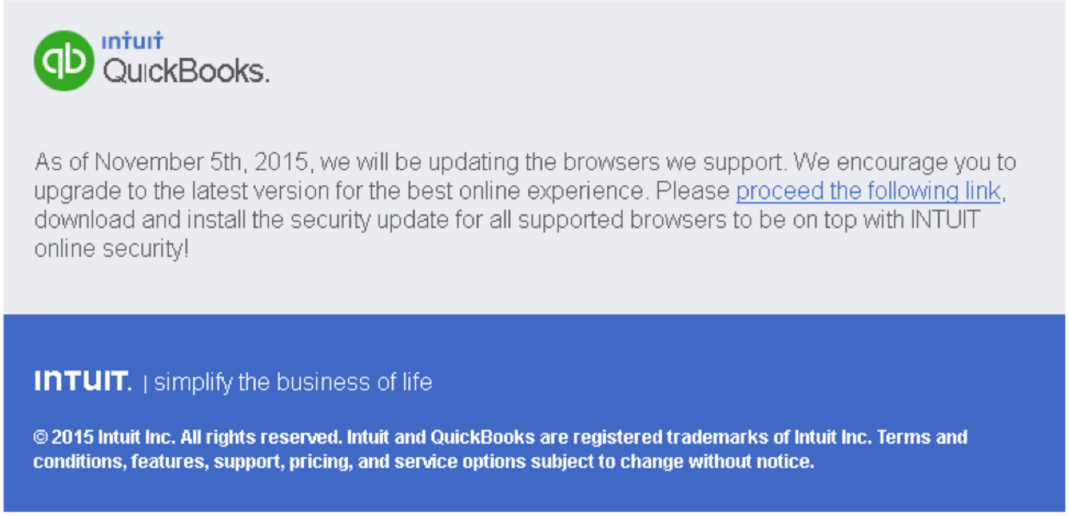
Invoice Details

Customer Billing

Microsoft

Microsoft
Word 2016

Figure 5: Malicious macro document that delivered Nymaim[19]



As of November 5th, 2015, we will be updating the browsers we support. We encourage you to upgrade to the latest version for the best online experience. Please proceed the following link, download and install the security update for all supported browsers to be on top with INTUIT online security!

© 2015 Intuit Inc. All rights reserved. Intuit and QuickBooks are registered trademarks of Intuit Inc. Terms and conditions, features, support, pricing, and service options subject to change without notice.

Figure 6: Spam to disguise Nymaim as an Intuit software update[20]

The Shift from Ransomware to Banking Trojans and the Emergence of GozNym

Nymaim's typical second-stage payload in its early years (2013-2015) was police ransomware. It locked victims' screens with a message that accused them of illegal activities, such as the downloading of copyrighted material or the viewing of child pornography, and instructed them to pay a fine. It displayed customized lock screens that mimicked the branding of various North American and European law enforcement agencies, based on a victim's ostensible location. The ransom note offered Romanian victims the opportunity to pay in either euros or Romanian currency, the latter of which was cheaper. This idiosyncrasy had previously appeared in other forms of police ransomware and may have reflected the recycling of code among threat actors.[21]

The shift from police ransomware to online banking attacks began in 2015. Nymaim had begun downloading a Gozi ISFB web injection dynamic link library (DLL) module to use in attacks on online banking sessions by November 2015.[22] Nymaim later began infecting victims with full second-stage Gozi ISFB payloads by February 2016.[23]

The hybrid GozNym banking Trojan was first detected in April 2016. It combines Nymaim's stealth and persistence features with a modified version of Gozi ISFB's web injection functionality. Nymaim operators may have obtained and recycled elements of Gozi ISFB source code from leaks, modified its web injection functionality, and integrated and recompiled it into the existing Nymaim source code base.[24] Accordingly, most anti-virus software vendors detect GozNym as Nymaim and not as a separate malware family or a variant of Gozi ISFB, as most of its non-banking behaviors reflect those of Nymaim, rather than Gozi. It may therefore be more accurate to describe GozNym as a variant of Nymaim than a variant of Gozi. GozNym samples have used some of the same command and control (C2) infrastructure as Nymaim samples, which further substantiates the belief that GozNym is a product of the Nymaim operators.[25]

Stealth Features

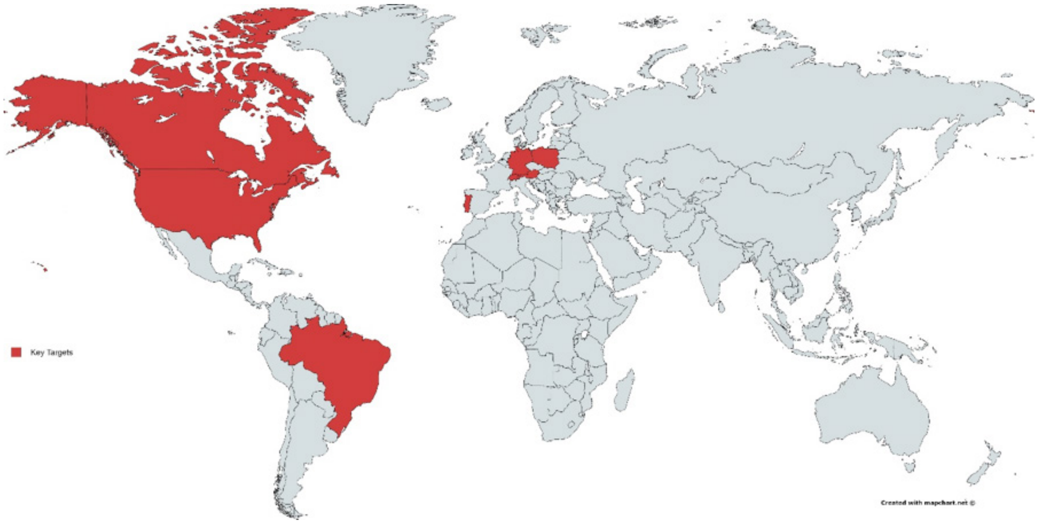
Early (2013) Nymaim samples concealed their C2 servers by communicating with them through a list of proxies hard-coded into the binary. It encrypted its normal traffic with RC4 encryption but added a second, mixed layer of RSA and custom encryption when it downloaded second-stage malware payloads.[26] By October 2015, Nymaim samples featured a domain generation algorithm (DGA).[27] As of April 2016, post-infection traffic for some Nymaim samples used the HTTPS, TCP, and UDP protocols,[28] while an April 2016 GozNym sample sent its traffic in the clear via HTTP.[29]

Other Nymaim stealth techniques include the obfuscation of control flow and API calls and the encryption of strings in the binary.[30] As of November 2015, Nymaim had begun to use a time check as an anti-analysis technique. The binary would not execute completely after a certain date–for example, two days after its distribution in the wild.[31] GozNym inherited this time check from Nymaim, and samples of it will not execute after an expiration date.[32]

Geographic Distribution and Targeting

Country-specific lock screens for victims of Nymaim's early (2013-2015) police ransomware covered 12 countries: the United States, Canada, Mexico, the United Kingdom, Ireland, the Netherlands, Norway, Germany, Austria, France, Spain, and Romania. The amount that it demanded from victims in the United States ($300) was approximately twice as high as the amounts that it demanded from victims in other countries, which averaged around $150.[33]

As of May 2015, Germany had the highest concentration of Nymaim infections by far (76%), with other significant concentrations in the United States (9%), Austria (8%), Poland (4%), and Portgual (3%).[34] Nymaim was also active in Switzerland as of August 2015.[35] As of March and early April 2016, the highest concentrations of GozNym infections were also in the United States, Austria, and Germany (in that order). Poland and Portugal also had high numbers of GozNym victims relative to the sizes of their respective populations but declined in relative significance as GozNym spread further beyond North America and Europe to developing and more populous countries in the Middle East, Latin America, South Asia, and Southeast Asia.[36]



The first configuration of the early GozNym samples that originally surfaced in April 2016 targeted 22 U.S. financial institutions and e-commerce platforms and two Canadian financial institutions.[37] A second GozNym configuration that surfaced later in April 2016 targeted 17 Polish banks, one Portuguese bank, and one U.S. bank. [38] A third GozNym configuration that targeted thirteen German financial institutions surfaced in August 2016.[39]

Conclusion

Nymaim highlights the importance of underground threat actor forums and markets both to the threat actors themselves and as a source of intelligence for the security community. In the absence of evidence that Nymaim is available in such underground communities, one can reasonably assess that its developer(s) retained exclusive access to it for their own attacks over the past three years. If so, the developer(s) have used it as the proprietary centerpiece of a criminal enterprise that otherwise depends heavily on products and services from other actors and external sources, both for its initial infection vectors and its second-stage payloads. Underground communities are typically where threat actors establish these vendor-client relationships or obtain malware source code via purchases or leaks.

Nymaim's shift away from ransomware and toward online banking attacks goes against the current trend toward the proliferation of new ransomware families and the growing numbers, scale, sophistication, and severity of ransomware attacks. Perhaps Nymaim operators decided that ransomware had already saturated the market, or that the ransomware bandwagon has left a vacuum in the market for online banking credentials to fill. Nymaim operators also never made the transition from police ransomware to crypto-ransomware that most ransomware attacks and operators have made. Police ransomware has since faded in significance and grown obsolete as crypto-ransomware, which encrypts files and holds them for ransom, has largely replaced it.

Nymaim attacks have acquired a clearer geographic focus since 2015, the year in which Nymaim operators shifted from ransomware to online banking attacks. This clearer focus may reflect the tendency of many financial institutions to serve customers in certain geographic areas. The focus on English-speaking North America and German-speaking Central Europe reflects the typical focus of criminal actors on wealthier markets. Nymaim operators' interest in Poland could reflect either the prevalence of such criminal actors in Eastern Europe, Poland's extensive economic ties to neighboring Germany, or some combination of both. The reason for the Nymaim operators' interest in Portugal, a smaller and less lucrative target, remains unclear.

Recommendations

- Prioritize the education of users with access to corporate bank accounts about social engineering threats. These users may be more susceptible to the common financial themes of malicious attachments and links in many criminal attacks, and the infection of their workstations with banking Trojans poses a greater risk of financial loss.
- Block users from enabling macros, especially when they are in Microsoft Office attachments to email messages from outside your corporate network. New features in Microsoft Office 2016 facilitate the blocking of macros in such higher-risk situations.
- If your anti-virus software detects a threat as Nymaim, remember that it might actually be either GozNym or Nymaim.
- Use the below indicators to block or detect Nymaim and GozNym attacks.

Indicators of Compromise (IOCs)

GozNym payloads (MD5)

2a9093307e667cdb71884ecc1b480245
f652ff6f745ac302e7067e5a347bb644
b954391bc225c662d4720bc8ae5f95cc
0058b5a2cbf64b536ea15c390e60de20
58d893c9074233d83ae694a180a28d01
c5ab408b9f710ebd63a515217a975274
20d6fe2353f3044d25d4fdc9f2872f39
e17a79a6f7c8fe7f920dad8cbcee3df0

Nymaim payloads (MD5)

d16b01a3b3852c0d64b5aa752e22e1be
f10cbacb7782ede3ab789e1b4fa21495
71022aab0b23aef9b69f6ac42d1c2c01
12abc10d3c37841f4f4f7e193b045f6b
563a1f54b9d90965951db0d469ecea6d
60b2009138d1b21c1b93b7093bc66109

Documents that download GozNym payloads (SHA256)

cf608be7dc6738dd178dc5a63bb21925e70800667a5876f2742bed59b5f6f5a1
ef4b06c20fae78d44c41402163d7624833fbbff4993d228682718b6b637fd637
ae56c3c196a60d380782a61d318065577b3f6abd04489c7c24d50fef1ed1429e
976ec8a4ed5026842ad397565c9ae1ee6911ffdd4007d2761e9b573e79f41384

Documents that download Nymaim payloads (SHA256)

ce0c220603d23fbb072f91a6a813c07e0c1d02559f54f9899d3d3be1db6d8851
617f3001d64cfc1edb3ccd70a084f888a34cb7f2e39d92e0685461baa23a4e5d
c788fd4cae05844344b04629d97be324d1f85dbefdfc8352489154341f888aa9
18e2461c250aaada1847b2aba8aef43f7686477f11b64e7597c325ee557f5128
3e522c5873f976078e2c31681771640c73ee8a4e192ecbbcf6fe4e8b3a486920
d78e20396efc39af29717d8dcceaf48a241ebd36a2f89d0c903ecf81fa9f5d0c
5cdf41ef8cc330a5ea7fa06de6e220afdd8c2d5b708041296801f45bcafa16e3
d4e3fb25f0d397967f1e88baffb97cfd6f40953d0c9f998d1c4694d1982d2d65
8efdfcf63f1dbfa9666bce23246f49c5788ec8c8edacc722038d9110375d89b5
e5c5385b79743ced00adebc0daae5fa619cf3836417bc2b0379f98a24f81c4bb
c0515052e8bc2e2772b29cbb694e72af9a6c2be8ebceba5766bcdaf26fe955da
b5b6b37f28dc16bbbac8df75af51f66436f7a4b4dec7ee3d911fb2601c1bb3b5
642420b08d6333b8cf48014b62c60f9bd1f51be4b3c00b6023e824987d177b73
4d0c14edfa616c0a5618b312f5ca90b3a29188288f35c5d8c1c2ae37ef11371f
a8ae681463b75470be8dc911f0cf7ca01a2eaea87005564263a5bbe38d652369

URLs for documents that download Nymaim payloads

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
hxxp://kompuser[.]com/system/logs/update/doc.php?r=download&id=INTUIT-Browser-up1247.zip

Domains, URLs, and IPs that host Nymaim payloads

160.153.16.52
46.249.54.179
traptractors[.]eu/system/logs/office.exe
banyoperdem[.]com/system/logs/office.exe
arabtradenet[.]com/info/content.dat
dalinumsdeli42[.]com/posts/dli506.exe
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 and GozNym C2 infrastructure

31.210.116.68
31.210.116.90
24.97.2.82
94.230.0.230
188.247.102.215
89.163.249.75
95.173.164.212
85.171.195.89
45.32.152.165
194.149.138.49
54.186.122.88
82.13.46.90
168.235.72.204
film-carpet-birth[.]com
beginninghang[.]com
kcrznhnlpw[.]com
mediapartnersallowallow[.]pw
hxxp://ytugctbfm.com/bewfa5ovkx/index.php
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
hxxp://onbrk[.]in/p7yqpgzemv/index.php

References

[1] L. Kessem, “Gozi Goes to Bulgaria–Is Cybercrime Heading to Less Charted Territory?” Security Intelligence, 18 August 2015 [Online]. Available: https://securityintelligence.com/gozi-goes-to-bulgaria-is-cybercrime-heading-to-less-chartered-territory/. [Accessed 12 May 2016].

[2] Staff, “Hybrid GozNym banking Trojan targets North American financial sector,” Deloitte TIA, 14 April 2016 [Online]. W-TN-EN-16-00265; Staff, “New version of GozNym banking Trojan, Deloitte TIA, 25 April 2016 [Online]. G-TN-EN-16-00290.

[3] L. Keshet and L. Kessem, "Meet GozNym: the banking malware offspring of Gozi ISFB and Nymaim," Security Intelligence, 14 April 2016. [Online]. Available: https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/. [Accessed 14 April 2016].

[4] S. Duquette, “The Home Campaign: overstaying its welcome,” We Live Security, 2 July 2013 [Online]. Available: http://www.welivesecurity.com/2013/07/02/the-home-campaign-overstaying-its-welcome/. [Accessed 22 April 2016].

[5] J. Boutin, “Nymaim: Browsing for trouble,” We Live Security, 23 October 2013 [Online]. Available: http://www.welivesecurity.com/2013/10/23/nymaim-browsing-for-trouble/. [Accessed 22 April 2016].

[6] Staff, “Dridex actors get in the ransomware game with Locky,” Proofpoint, 16 February 2016 [Online]. Available: http://proofpoint.com/us/threat-insight/post/Dridex-Actors-Get-In-the-Ransomware-Game-With-Locky. [Accessed 22 April 2016].

[7] Staff, “What Is Old Is New Again - Nymaim Moves Past Its Ransomware Roots,” Proofpoint, 21 April 2016 [Online]. Available: https://www.proofpoint.com/us/what-old-new-again-nymaim-moves-past-its-ransomware-roots-0. [Accessed 21 April 2016].

[8] M. Mesa, “Phish Scales: Malicious Actor Combines Personalized Email, Variety of Malware to Target Execs,” Proofpoint, 5 April 2016 [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/phish-scales-malicious-actor-target-execs. [Accessed 21 April 2016].

[9] Staff, “Malicious Macros Add Sandbox Evasion Techniques to Distribute New Dridex,” Proofpoint, 2 June 2016 [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/malicious-macros-add-to-sandbox-evasion-techniques-to-distribute-new-dridex. [Accessed 9 June 2016].

[10] J. Boutin, “Nymaim – obfuscation chronicles,” We Live Security, 26 August 2013 [Online]. Available: http://www.welivesecurity.com/2013/08/26/nymaim-obfuscation-chronicles/. [Accessed 22 April 2016]; Staff, “What Is Old Is New Again - Nymaim Moves Past Its Ransomware Roots,” Proofpoint, 21 April 2016 [Online]. Available: https://www.proofpoint.com/us/what-old-new-again-nymaim-moves-past-its-ransomware-roots-0. [Accessed 21 April 2016]; L. Keshet and L. Kessem, "Meet GozNym: the banking malware offspring of Gozi ISFB and Nymaim," Security Intelligence, 14 April 2016. [Online]. Available: https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/. [Accessed 14 April 2016].

[11] Hasherezade, “No money, but Pony! From a mail to a Trojan horse,” Malwarebytes, 19 November 2015 [Online]. Available: https://blog.malwarebytes.org/threat-analysis/2015/11/no-money-but-pony-from-a-mail-to-a-trojan-horse/. [Accessed 12 May 2016]; I. Palmer, “Pony loader 2.0 steals credentials and bitcoin wallets: source code for sale,” Damballa, 24 June 2014 [Online]. Available: https://www.damballa.com/pony-loader-2-0-steals-credentials-bitcoin-wallets-source-code-sale/. [Accessed 12 May 2016].

[12] C. Longmore, “Mystery INTUIT QuickBooks” spam leads to unknown malware,” Dynamoo Blog, 18 November 2015 [Online]. Available: http://blog.dynamoo.com/2015/11/mystery-intuit-quickbooks-spam-leads-to.html. [Accessed 22 April 2016].

[13] Staff, “Malicious Word doc downloads Nymaim and info stealer,” Broad Analysis 19 April 2016 [Online]. Available: http://www.broadanalysis.com/2016/04/19/malicious-word-doc-downloads-nymaim-and-info-stealer/. [Accessed 22 April 2016].

[14] M. Mesa, “Phish Scales: Malicious Actor Combines Personalized Email, Variety of Malware to Target Execs,” Proofpoint, 5 April 2016 [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/phish-scales-malicious-actor-target-execs. [Accessed 21 April 2016].

[15] Staff, “Malicious Word Doc sends Nymaim and SSL data Exfiltration,” Broad Analysis, 12 April 2016 [Online]. Available: http://www.broadanalysis.com/2016/04/12/malicious-word-doc-sends-nymaim-and-ssl-data-exfiltration/. [Accessed 22 April 2016].

[16] Staff, “What Is Old Is New Again - Nymaim Moves Past Its Ransomware Roots,” Proofpoint, 21 April 2016 [Online]. Available: https://www.proofpoint.com/us/what-old-new-again-nymaim-moves-past-its-ransomware-roots-0.

[17] Staff, “Malicious Macros Add Sandbox Evasion Techniques to Distribute New Dridex,” Proofpoint, 2 June 2016 [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/malicious-macros-add-to-sandbox-evasion-techniques-to-distribute-new-dridex. [Accessed 9 June 2016].

[18] M. Mesa, “Phish Scales: Malicious Actor Combines Personalized Email, Variety of Malware to Target Execs,” Proofpoint, 5 April 2016 [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/phish-scales-malicious-actor-target-execs. [Accessed 21 April 2016].

[19] Staff, “Malicious Word doc downloads Nymaim and info stealer,” Broad Analysis 19 April 2016 [Online]. Available: http://www.broadanalysis.com/2016/04/19/malicious-word-doc-downloads-nymaim-and-info-stealer/. [Accessed 22 April 2016].

[20] C. Longmore, “Mystery INTUIT QuickBooks” spam leads to unknown malware,” Dynamoo Blog, 18 November 2015 [Online]. Available: http://blog.dynamoo.com/2015/11/mystery-intuit-quickbooks-spam-leads-to.html. [Accessed 22 April 2016].

[21] J. Boutin, “Nymaim: Browsing for trouble,” We Live Security, 23 October 2013 [Online]. Available: http://www.welivesecurity.com/2013/10/23/nymaim-browsing-for-trouble/. [Accessed 22 April 2016].

[22] L. Keshet and L. Kessem, "Meet GozNym: the banking malware offspring of Gozi ISFB and Nymaim," Security Intelligence, 14 April 2016. [Online]. Available: https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/. [Accessed 14 April 2016].

[23] Staff, “What Is Old Is New Again - Nymaim Moves Past Its Ransomware Roots,” Proofpoint, 21 April 2016 [Online]. Available: https://www.proofpoint.com/us/what-old-new-again-nymaim-moves-past-its-ransomware-roots-0. [Accessed 21 April 2016].

[24] L. Keshet and L. Kessem, "Meet GozNym: the banking malware offspring of Gozi ISFB and Nymaim," Security Intelligence, 14 April 2016. [Online]. Available: https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/. [Accessed 14 April 2016].

[25] Staff, “GozNym malware,” Team Cymru, 2 May 2016 [Online]. Available: https://blog.team-cymru.org/2016/05/goznym-malware/. [Accessed 3 May 2016].

[26] J. Boutin, “Nymaim: Browsing for trouble,” We Live Security, 23 October 2013 [Online]. Available: http://www.welivesecurity.com/2013/10/23/nymaim-browsing-for-trouble/. [Accessed 22 April 2016].

[27] Staff, “Neue DGA domains für Matsnu/Nymaim aktiv,” Bits, Bytes, and My 5 Cents, 13 October 2015 [Online]. Available: http://blog.encodingit.ch/tag/nymaim/. [Accessed 22 April 2016].

[28] Staff, “Malicious Word Doc sends Nymaim and SSL data Exfiltration,” Broad Analysis, 12 April 2016 [Online]. Available: http://www.broadanalysis.com/2016/04/12/malicious-word-doc-sends-nymaim-and-ssl-data-exfiltration/. [Accessed 22 April 2016].

[29] Staff, “GozNym malware,” Team Cymru, 2 May 2016 [Online]. Available: https://blog.team-cymru.org/2016/05/goznym-malware/. [Accessed 3 May 2016].

[30] J. Boutin, “Nymaim – obfuscation chronicles,” We Live Security, 26 August 2013 [Online]. Available: http://www.welivesecurity.com/2013/08/26/nymaim-obfuscation-chronicles/. [Accessed 22 April 2016].

[31] Staff, “Nymaim malware obfuscation and system time check,” Neutralize Cyber Threats, 1 December 2015 [Online]. Available: http://www.neutralizethreat.com/2015/12/nymaim-malware-obfuscation-and-system.html. [Accessed 22 April 2016].

[32] Staff, “GozNym malware,” Team Cymru, 2 May 2016 [Online]. Available: https://blog.team-cymru.org/2016/05/goznym-malware/. [Accessed 3 May 2016].

[33] J. Boutin, “Nymaim: Browsing for trouble,” We Live Security, 23 October 2013 [Online]. Available: http://www.welivesecurity.com/2013/10/23/nymaim-browsing-for-trouble/. [Accessed 22 April 2016].

[34] N. Periquito, “Germany Meets Nymaim,” Anubis Networks, 26 May 2015 [Online]. Available: http://blog.anubisnetworks.com/blog/germany-meets-nymaim. [Accessed 22 April 2016].

[35] Staff, “Nymaim in der Schweiz wieder aktiv,” Bits, Bytes, and My 5 Cents, 24 August 2015 [Online]. Available: http://blog.encodingit.ch/2015/08/nymaim-in-der-schweiz-wieder-aktiv/.
[Accessed 22 April 2015].

[36] Staff, “GozNym malware,” Team Cymru, 2 May 2016 [Online]. Available: https://blog.team-cymru.org/2016/05/goznym-malware/. [Accessed 3 May 2016].

[37] L. Keshet and L. Kessem, "Meet GozNym: the banking malware offspring of Gozi ISFB and Nymaim," Security Intelligence, 14 April 2016. [Online]. Available: https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/. [Accessed 14 April 2016].

[38] L. Kessem, “Time is Money: GozNym Launches Redirection Attacks in Poland,” Security Intelligence, 25 April 2016 [Online]. Available: https://securityintelligence.com/time-is-money-goznym-launches-redirection-attacks-in-poland/.
[Accessed 25 April 2016].

[39] L. Kessem, “GozNym’s Euro Trip: Launching Redirection Attacks in Germany,” Security Intelligence, 23 August 2016 [Online]. Available: https://securityintelligence.com/goznyms-euro-trip-launching-redirection-attacks-in-germany/. [Accessed 24 August 2016].

About Deloitte Threat Studies

These studies are the result of detailed research conducted by our Threat Analysis & Research (TAR) team on an ongoing threat or emerging threat trend, typically focusing on a specific threat actor or a specific technical issue that is persistent over time. It contains detailed information on adversary TTPs and IOCs.

About Deloitte's Threat Analysis & Research (TAR)

TAR is delivered as an annual subscription service that provides client-specific threat insights and business impact through collection & analysis of data across numerous sources of information including darkweb, criminal forums, third-party intelligence or other sources. Our professionals have advanced language skills and regional knowledge, and extensive intelligence experience from law enforcement, government, military, and cyber intelligence companies.

Secure.Vigilant.Resilient.™

To grow, streamline and innovate, many organizations have difficulty keeping pace with the evolution of cyber threats. The traditional discipline of IT security, isolated from a more comprehensive risk-based approach, may no longer be enough to protect you. Through the lens of what's most important to your organization, you must invest in cost-justified security controls to protect your most important assets, and focus equal or greater effort on gaining more insight into threats, and responding more effectively to reduce their impact. A Secure.Vigilant.Resilient. cyber risk program can help you become more confident in your ability to reap the value of your strategic investments.

- BEING SECURE means having risk-focused defenses around what matters most to your mission.
- BEING VIGILANT means having threat awareness to know when a compromise has occurred, or may be imminent.
- BEING RESILIENT means having the ability to regain ground when an incident does occur.

Deloitte.

This report contains general information only and Deloitte is not, by means of this report, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This report is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. -

Deloitte shall not be responsible for any loss sustained by any person who relies on this report.