ARTICLE OVERVIEW

Antivirus software detects GozNym hybrid as Nymaim variant

GozNym samples resolve domains, do not connect to IPs returned. Separate IP used for
HTTP comms.

C2 channel for GozNym appears to be HTTP POST requests, in line with Nymaim-based
origins

Recent active related C2s at 194.149.138.49, 54.186.122.88, 82.13.46.90, 168.235.72.204 and
domain ytugctbfm[.]com used

IP85.171.195.89 likely C2 for late March/early April 2016 campaign

Late March/early April 2016 campaign appears to primarily target US, AT, DE

Campaigns are time-limited and samples will not run if system clock is outside a pre-set
date range

Recent reports have indicated the emergence of a hybrid of the Nymaim loader malware and the Gozi financial Trojan, dubbed 'GozNym'. This report analysis hashes associated with GozNym and identifies associated samples, domains and IPs.
Open sources provide a number of hashes of malware samples claimed to be GozNym. These are shown below.

Sample MD5
2a9093307e667cdb71884ecc1b480245
f652ff6f745ac302e7067e5a347bb644
b954391bc225c662d4720bc8ae5f95cc
0058b5a2cbf64b536ea15c390e60de20
58d893c9074233d83ae694a180a28d01
c5ab408b9f710ebd63a515217a975274

Table 1- Open source GozNym MD5s

As of 18 April 2016, there is no specific 'GozNym' signature provided by any antivirus vendor, with most vendors detecting the above samples as Nymaim variants. Similar to Nymaim, GozNym samples and campaigns appear to be time-limited: i.e. samples will not run outside of a predefined date range.

Note: as a result of this behaviour, this report references a number of historic sandbox runs from early April 2016 to present.

Sample 2a90…0245 (identified by IBM) is detected by Microsoft as 'TrojanDownloader:Win32/Nymaim' and Ikarus as 'Trojan-Banker.Gozi'. At the time of writing, this is the only sample recorded displaying these attributes.

In a PCAP obtained from VirusTotal, dating from 6 April 2016, sample c5ab4…5274 (identified by IBM1) was observed to resolve the domain 'kcrznhnlpw[.]com' and make an HTTP POST request to '85.171.195.89/zdf3nb6i/index.php'. The header of this POST request is shown below.

```
POST /zdf3nb6i/index.php HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Host: kcrznhnlpw[.]com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1;
Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3)
Content-Length: 11853
```

Figure 1 – GozNym/Nymaim HTTP POST request header

This HTTP POST activity is in-line with behaviour previously associated with Nymaim.

The DNS query response for 'kcrznhnlpw[.]com' in the session analysed provided four

IP addresses:

IP	AS	Details
59.116.23.197	3462	HINET Data Communication Business Group, TW
165.203.213.15	-	Associates Bancorp (ASSOCI-1), US
21.221.249.200	-	DoD Network Information Center, US
33.38.160.238	-	DoD Network Information Center, US

Table 2 – DNSRRs for 'kcrznhnlpw[.]com' (6 April 2016)

Note that the POST request ostensibly made to 'kcrznhnlpw[.]com' shown above in Figure 1 was sent to 85.171.195.89 (AS21502 – ASN-NUMERICABLE NC Numericable S.A., FR), not one of the addresses in Table 2.
The reason for this behaviour is unclear, although it may imply that a form of transform is being applied to the IPs returned in the DNS response.

Searching for samples which perform DNS queries for 'kcrznhnlpw[.]com' returns two additional samples:

Sample MD5
47bd2478feb9cb0c08f7e716c94cc8c8
f1a12884b999b9e572f91a94043d6e01

Table 3 – Malware samples querying 'kcrznhnlpw[.]com'

Sample 47bd2478feb9cb0c08f7e716c94cc8c8 was sandboxed on 8 April 2016, at which point in time the DNS record for 'kcrznhnlpw[.]com' had been modified (see Table 4 below).

IP	AS	Details	Changed
59.116.23.197	3462	HINET Data Communication Business Group, TW	NO
165.203.213.15	-	Associates Bancorp (ASSOCI-1), US	NO
21.26.242.199	-	DoD Network Information Center, US	YES
33.38.160.238	-	DoD Network Information Center, US	NO

Table 4 – DNSRRs for 'kcrznhnlpw[.]com' (8 April 2016)

This may suggest a change in infrastructure around this time period.

The implications of the target IP used for the HTTP POST requests not changing, despite a change in the returned DNSRRs, are unclear. While it may suggest that the

DNSRRs are used for something other than a 'transform' into the target IP, it may simply mean that the IP transformed into 85.171.195.89 is one of the three to remain unchanged.

This sample then made HTTP POST requests to the IP addresses shown in Table 5. At the time, both of these addresses were responsive and returned data.

IP	AS	Details
85.171.195.89	21502	ASN-NUMERICABLE NC Numericable S.A., FR
5.154.240.145	50908	ASTIMPIT Astimp Consulting SRL, RO

Table 5 – HTTP POST target IPs for 47bd2478feb9cb0c08f7e716c94cc8c8

Searching based on 85.171.195.89 – the common destination IP for the HTTP POST requests – reveals one additional sample, also identified by antivirus products as Nymaim.

Sample MD5
f232cffa7802e54141f6f46691039e4b

Table 6 – Malware samples with flows to 85.171.195.89

The lack of specific antivirus signatures for GozNym coupled with many of its behaviour characteristics being akin to those of Nymaim are significant limiting factors when attempting to differentiate the malware from 'standard' Nymaim/Gozi samples. Passive DNS results identified other domains that have historically resolved to the same IP addresses listed in table 4. These domains showed similar random letter pattern as visible in Table 7.

Domain	165.203.213.15	21.26.242.199	33.38.160.238	59.116.23.197	9.116.23.197
kcrznhnlpw[.]com	X	X	X	X	
wlefihdmss[.]com	X	X	X	X	
mbcqjsuqsd[.]com	X	X	X	X	
humzka[.]com	X		X		X
ibfvpi[.]com	X	X	X		
jiupjod[.]com	X	X	X		
krlsloeohxex[.]com	X		X	X	
mlvrkarzbg[.]com	X	X	X		
npmuzz[.]com	X		X	X	
pjhwvateyxy[.]com	X	X	X		
ytugctbfm[.]com	X	X	X		
ssksxalx[.]com	X		X	X	
ykyru[.]com	X		X		

Table 7 – PDNS matrix for 'kcrznhnlpw[.]com' IPs

All of the domains listed in Table 7 appear to have been registered via Key-Systems GmbH. Table 8 lists registration dates and DNS records for these domains as of 20 April 2016.

Domain	WHOIS Creation	WHOIS Last Update	DNS Records
ykyru[.]com	2016-03-14	2016-03-27	-
krlsloeohxex[.]com	2016-03-25	2016-03-30	-
mbcqjsuqsd[.]com	2016-03-26	2016-03-30	-
humzka[.]com	2016-03-27	2016-04-01	-
npmuzz[.]com	2016-03-30	2016-04-07	-
sskxsxalx[.]com	2016-03-30	2016-04-06	-
pjhwvateyxy[.]com	2016-04-03	2016-04-09	-
kcrznhnlpw[.]com	2016-04-04	2016-04-11	-
ibfvpi[.]com	2016-04-06	2016-04-06	102.247.192.26
			98.45.51.8 184.11.83.2 108.222.64.168
wlefihdmss[.]com	2016-04-07	2016-04-07	102.247.192.26 108.222.64.168 184.11.83.2 98.45.51.8
jiupjod[.]com	2016-04-09	2016-04-17	-
mlvrkarzbg[.]com	2016-04-13	2016-04-20	-
ytugctbfm[.]com	2016-04-17	2016-04-17 *(Query: 2016-04-20)*	108.222.64.168 102.247.192.26 98.45.51.8 184.11.83.2
		2016-04-17 *(Query: 2016-04-21)*	210.53.31.233 98.45.51.8 70.58.60.21 90.253.197.36

Table 8 – Registration & DNS details for domains associated with 'kcrznhnlpw[.]com' IPs

No malware samples have been observed contacting the IPs in Table 8 to date. This is in line with the observations made about the early-April DNSRRs associated with 'kcrznhnlpw[.]com'.

The results shown in Table 8 suggest that there are currently at least three active controllers associated with this campaign. Note that the three domains with associated DNS records as of 20 April 2016 return the same four IP addresses and appear to have been registered on the same day as one of the other associated domains was 'updated'.

Two malware samples (Table 9) were identified resolving the domain 'ytugctbfm[.]com'. In line with previously recorded Nymaim/GozNym behaviour, these samples were observed making HTTP POST requests to '/ub3w5stq/index.php' on the IPs in Table 10 and Table 11. All four of these IPs were responsive and returned data.

Sample MD5
44d09eac8cf488000fb8ab3585789b5b
2cd713ad63b5d9fe53000f2362d85fc9

Table 9 – Malware samples querying 'ytugctbfm[.]com'

IP	AS	Details
82.13.46.90	5089	NTL Virgin Media Limited, GB
168.235.72.204	3842	RAMNODE - RamNode LLC, US

Table 10 – HTTP POST target IPs for 44d09eac8cf488000fb8ab3585789b5b

IP	AS	Details
194.149.138.49	5379	MK-UKIM-AS Univerzitet _Sv. Kiril i Metodij_, MK
54.186.122.88	16509	AMAZON-02 - Amazon[.]com, Inc., US

Table 11 – HTTP POST target IPs for 2cd713ad63b5d9fe53000f2362d85fc9

Of the domains which appear inactive as of the time of writing, three malware samples were identified resolving the domain 'ykyru[.]com' and one resolving the domain 'humzka[.]com'. The details of these samples are listed in Table 12.

Sample MD5	Domain	First Seen
57944ba9a7ebdd2ced0f53779582ea73	ykyru[.]com	2016-03-24
9c17bd1dac02ff0fb5608d388a4f0797	ykyru[.]com	2016-03-25
c41ffc1fd6e3f5157181b6e45f45f4fe	ykyru[.]com	2016-03-24
1ba77419aacbd0360ebc24e06cf2bb1c	humzka[.]com	2016-03-31

Table 12 – Malware samples contacting domains from Table 7

The samples associated with 'ykyru[.]com' were identified by antivirus products as Nymaim, while the sample associated with 'humzka[.]com' was identified as DDoS:Win32/Nitol.D (Microsoft) or Backdoor.Win32.Androm.jjha (Kaspersky). PCAP results for samples 57944…ea73 and 1ba77…bb1c generated similar HTTP POST requests directed towards mis-matched IP/domain combinations. Table 13 and Table 14 show the DNSRR entries for 'ykyru[.]com' and 'humzka[.]com', respectively.

IP	AS	Details
21.45.165.216	-	DoD Network Information Center, US
42.65.42.11	17421	EMOME-TW Long Distance & Mobile Business Group, TW
208.104.191.196	14615	ROCK-HILL-TELEPHONE - Comporium, Inc, US
165.203.213.15	-	Associates Bancorp (ASSOCI-1), US

Table 13 – DNSRRs for 'ykyru[.]com' (24 March 2016)

IP	AS	Details
33.38.160.238	-	DoD Network Information Center, US
185.38.68.7	199999	BNNIT AKVA group Software AS, NO
21.221.249.200	-	DoD Network Information Center, US
165.203.213.15	-	Associates Bancorp (ASSOCI-1), US
228.26.91.81	-	RFC 3171 - Multicast

Table 14 – DNSRRs for 'humzka[.]com' (31 March 2016)

Communications with Command and Control (C2) Servers on 80/TCP can potentially provide insight into victim distribution for this campaign. Summary data is shown below, with Figure 2 showing the top twenty country codes affected and Figure 3 the top twenty ASes, both calculated by the number of unique IPs observed.

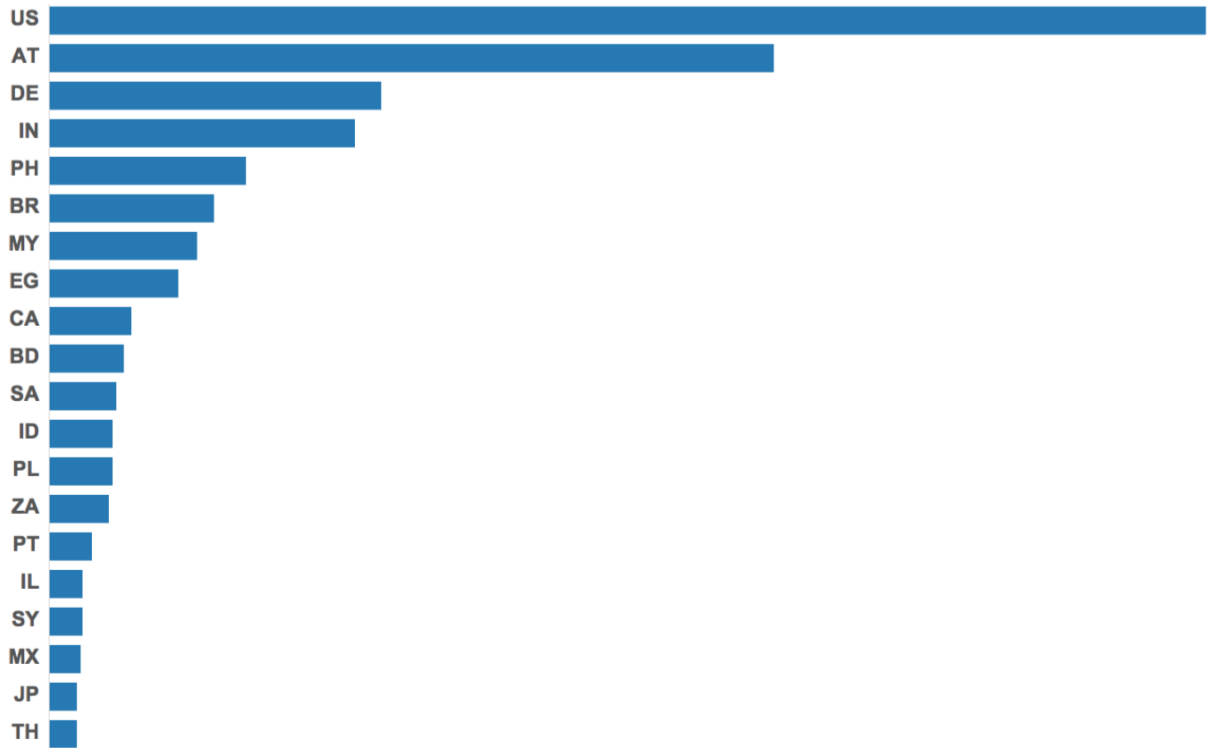

Figure 2 – Top 20 country codes contacting C2 on 80/TCP (by unique IP)

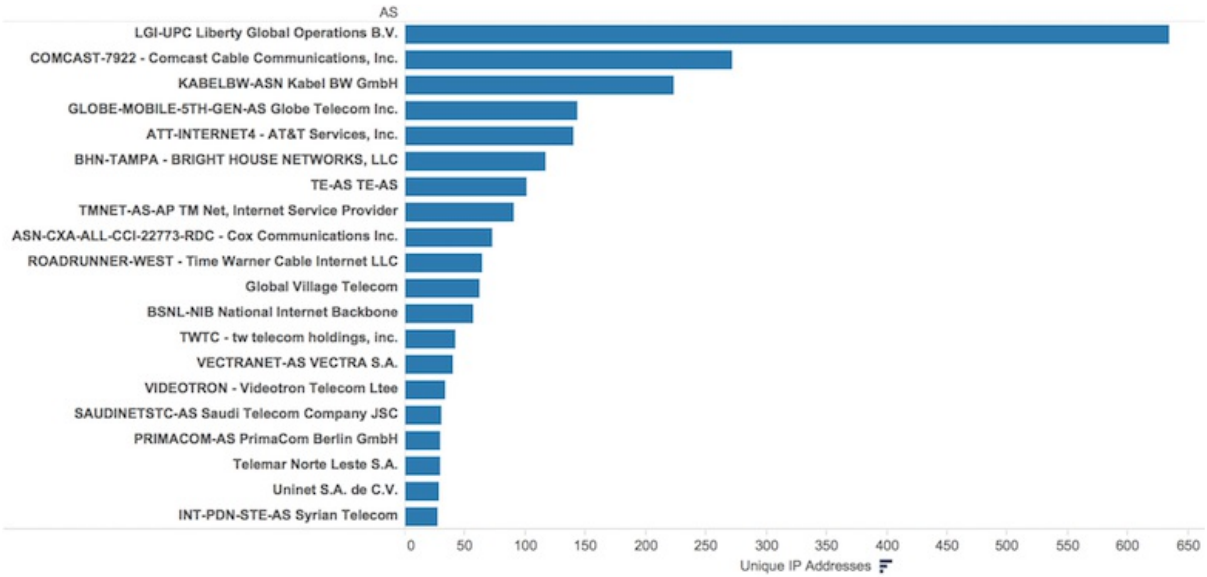

Figure 3 – Top 20 ASes contacting C2 on 80/TCP (by unique IP)

It should be noted that the IPs recorded contacting C2 on 80/TCP appear to be predominantly consumer broadband connections likely using dynamic IP allocation. As such, the numbers above should be treated as indicative only.

#GOZNYM

THREATS

SHARE: