



Jon DiMaggio [Follow](#)

Jon DiMaggio a Senior Threat Intelligence Analyst at Symantec with the Security Response wh...
May 31 · 10 min read

Operation Bachosens: A detailed look into a long-running cyber crime campaign

A recent investigation into a unique malware attack on an automotive parts supplier in China ended quite unexpectedly. As well as discovering rarely-used malware techniques, we also discovered unexpected motivations of the individual who is likely behind the attacks, and the great lengths he went to for relatively meager gain.



In March 2016, Symantec's automated attack notification systems, which run on our vast telemetry, identified a potentially interesting targeted attack. One of the initial interesting attributes of the attack was the small number of organizations and regions targeted. Our initial triage found a custom keylogger, along with two unknown suspicious files.

Hash	Filename	Note
0A8837790FC569A060CD5599E66FA046	Positive.dll	Unknown (possible backdoor)
4770941FAE573D06389351B36D589B48	Sens.dll	Unknown (possible backdoor)
14CFEBE12DCCA5E5BB7C3EE2BEC06A0A	stor64.dll	HackTool (64 bit keylogger)

Part 1: Following the malware

Analyzing the unknown samples, we confirmed they were a new backdoor Trojan that Symantec now detects as Trojan.Bachosens. Once the Bachosens malware is dropped on the victim computer, it creates a number of files which, in this instance, were designed to masquerade as the legitimate Java application on the target's computer to avoid detection:

%AppData%\Java\jusched.exe

%CommonProgramFiles%\java\jusched.exe

%CommonProgramFiles%\java\java update\jusched.exe

%CommonProgramFiles%\jusched.exe

%System%\sens.dll

%System%\stor64.dll

%System%\stor32.dll

Trojan.Bachosens then creates a registry entry so that it remains persistent on the computer and runs every time Windows starts:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\JavaUpdater = "[PATH TO MALWARE]\jusched.exe -v"

Both a 32 bit and a 64 bit keylogger were also identified being used in these attacks, depending on the target's environment. This was our first clue that the attacker was tailoring their tools and malware specifically for targets' environments. The keylogger was not dropped by the malware, so we suspect it is pushed manually by the attacker to systems of interest after the initial infection.

Once we had this information, the next step was to uncover the communication protocol of the backdoor. Right away, we discovered the backdoor used a domain generation algorithm (DGA). A DGA causes the command and control (C&C) server that the threat communicates with to change depending on the current date. This makes shutting down the attacker's infrastructure more difficult.

Some malware will generate hundreds or thousands of possible C&C domains as part of their DGA. Oddly, the Bachosens attacker developed

his malware to only generate 13 domains per year. Only two of the 13 domains are active at any given time: one domain that changes each month, and another that is static for the entire year.

For the monthly changing domain, Bachosens' DGA generates a predefined number of random characters seeded by the current date and pairs them with a free Dynamic DNS (DDNS) provided root domain:



For the yearly domain, Bachosens does the same, but ads .com rather than a static root domain.

Once we figured out this algorithm, we were able to generate all the domains for 2016 and 2017.

Domain	Month	Year
5nru85507oelijmi7ji2h0sq16z.xxuz.com	1	2016
4ha60cpg39nlhs8nsh33rmlu10z.xxuz.com	2	2016
j4lvab2ct01dihmd50jcd6dfp2z.xxuz.com	3	2016
4sio24i6ocpt1mveubiodbs3n4z.xxuz.com	4	2016
f9tfjn4b4kb3r0uq1dsef60jo4z.xxuz.com	5	2016
56r1j68pgvr4f2377etvm2io5z.xxuz.com	6	2016
u4070o5imekk3eqatkc95gs35z.xxuz.com	7	2016
f6279kvr98j592tkvhs5orj0z.xxuz.com	8	2016
13bm\text{v}qdr1ju64dqm6n8877hbo0z.xxuz.com	9	2016
832v1hda31sqfcl5bh81lmqk74z.xxuz.com	10	2016
kc591pa2ao7g4skkdaklcm7a71z.xxuz.com	11	2016
iujr13jeik4fpcbm20lram6dr6z.xxuz.com	12	2016
www.gf8ealht9d22g0ul8iu7evar74z.com	-	2016
uuls5pisqih6cv62h7m4mim530z.xxuz.com	1	2017
fkvehgcqlis081l1kocfbsjr77z.xxuz.com	2	2017
59vbs0bm040t9vgeqdlvje3l3z.xxuz.com	3	2017
lo405klrt90r8g75anljp22gs4z.xxuz.com	4	2017
gufm1p8gd7lm8r52kfntoa9ma4z.xxuz.com	5	2017
47j7b8ljt4cd727g2nnetkb244z.xxuz.com	6	2017
c798hldn2bjr0bs8sf2acn1t2z.xxuz.com	7	2017
n265sdakhe4em256tiqukk7ad5z.xxuz.com	8	2017
hv3teh46b1597b5av2n953r6h5z.xxuz.com	9	2017
ttb6clusnibu9a403g4r3kcqd3z.xxuz.com	10	2017
0h7nj556ld4qgjvpfetu0rrmv4z.xxuz.com	11	2017
02vks8oh0pu705chkjl5h0uq65z.xxuz.com	12	2017
www.9uaf5kdufm4non9f20rvpn0pt4z.com	-	2017

However, even after determining the threat used a DGA, we still had not fully uncovered the backdoor's C&C protocol. What we discovered next was not only unexpected, but became the catalyst for us to dig further.

Covert channels

Most backdoors use HTTP or HTTPS for communicating with their C&C servers, but this malware was communicating over DNS, ICMP, and HTTP protocols.

Our analysis showed the attacker actually coded the malware to attempt DNS (domain name system) communication first, switching to alternative methods only when necessary. DNS is the protocol used to translate domain names (example.com) into IP addresses (127.0.0.1). Using DNS for C&C communication has been documented previously, such techniques were seen being used in malware found in the Shadow Brokers leak, but it is rare.

In this case, the malware sends data encoded within the domain name to the DNS server and receives data from the attacker in the DNS response packet. DNS response records can provide multiple IP addresses and Bachosens relies on DNS AAAA response records. An AAAA response contains the requested domain's 128-bit IPv6 address. Instead of a valid IPv6 address, the address is encoded data from the attacker. Below is an example of the DNS traffic seen in the initial communication:

```
2016-08-08 17:26 2016-08-08 17:26 lok4723peoi8n1c0mk23rtmc91z.ostin.su (rrset) AAAA
d13:8355:57fe:3f93:7c8a:d406:e947:7c04, a96a:61c:1798:56ee:5a13:4954:1146:f105 2
```

The information transmitted in the initial communications from the malware to the DNS server includes an attacker-determined "Infection ID" (decoded below), along with the infection date.

So, for example, "lok4723peoi8n1comk23rtmc91z" is decrypted to "oc23ca440908c1e80301020000000000", which can be decoded into the "infection id" and infection date below:

nonce = oc

cksum = 23ca (verification PASS)

infection_id = c1080944

infection_year = 2016

infection_month = 8

infection_day = 8

infection_random = 0944

sid_relative_identifier = 1000

request_kind = 0201

padding_size = 0

request_sequence = 00000000

The DNS server responds back to the malware with a provided “session ID” and an RSA-encrypted communication channel is established over the same protocol where the victim’s environment, including operating system, computer name, and user name, is sent to the attacker.

The malware can perform this handshake and session establishment in a similar manner using DNA A records, DNS TXT records, ICMP Echo packets, and HTTP. After the communication channel session is established, the attacker has been seen to change protocols. For example, the attacker can instruct the malware to change from DNS to ICMP by sending the command “conn icmp <id>”.

While DNS is considered a covert method of communication, once we discovered it was being used we could search for historical DNS request and response records and decode the infection ID associated with each target and the precise infection date. This allowed us to build an accurate timeline based on the attacker’s own metrics. Through this process we were able to determine the adversary was active and present on the automotive victim’s network from December 2016 through February 2017.

The historic DNS records also confirmed attempted attacks on two other organizations: a commercial airline and an organization involved in the online entertainment industry.

While analyzing the malware we also came across an interesting aspect that could provide support for attribution. Russian strings for data sizes

were used. For example, 6 and r6 were found in the binary, which are the Russian equivalents of bytes (B) and gigabytes (GB).

Part 2: Determining attacker motivation

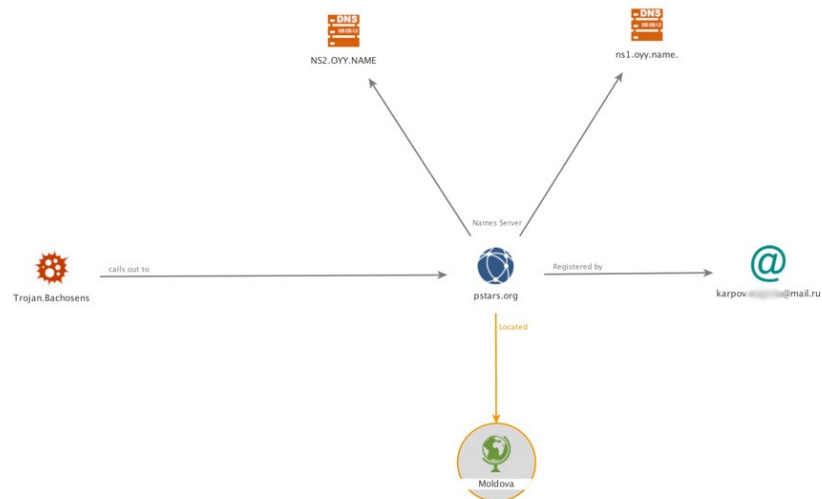
At this point in the investigation, we had a solid grasp of the malware features, including its unique communication protocol. However, the limited and diverse targets of an automotive parts supplier, an airline, and an online entertainment organization were puzzling. The automotive parts supplier was especially worrisome in the context of the recent Vault 7 leaks, which describe automobile hacking by a likely nation state. Understanding the objective of these attacks and who else may be a target was necessary. The following were the likely scenarios:

1. Could this be corporate espionage in which intellectual property is being stolen for the advantage of a competing firm?
2. Could this be a financially motivated cyber crime gang with the ability to develop or purchase unique undetected malware?
3. Could this be a nation-state attacker with a sabotage motivation?

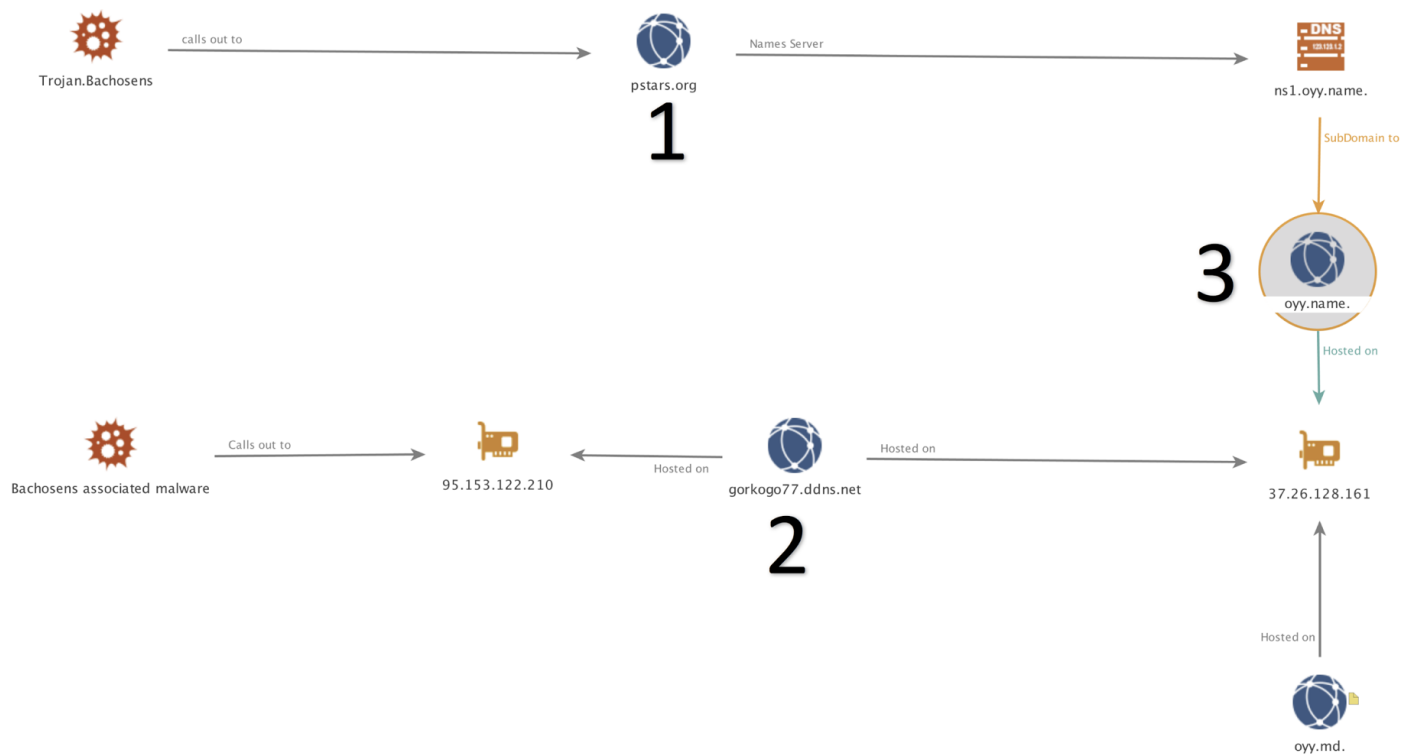
Through our reconstructed infection timeline, we were able to see what systems the adversary spent the most time on and noticed a reoccurring theme in the targets of interest. The systems in which the attacker spent the most time were automotive technology developer systems. Of the developer systems, the primary technology that appeared to be of interest to the attacker involved the development of a very specific automotive diagnostic technology. This technology is loaded into handheld diagnostic devices and sold to automotive repair shops globally. To protect the victims we are masking the technology and product name and will refer to it as “Diag-1000” for the remainder of the article.

Part 3: Attacker infrastructure and IOC ties

In addition to understanding the attack methods and victim profiles, analyzing the attacker’s infrastructure can provide potential attribution clues. The earliest known Bachosens keylogger from December 2013 did not rely on a DGA to generate the C&C domain but instead connected to the hardcoded domain of “pstars.org”. As seen in the diagram below, pstars.org used the name servers ns1.oyy[.]name & ns2.oyy[.]name.



At this point in the investigation, we had more than 70 samples we had analyzed made up of two versions of the Bachosens Trojan and two versions of the keyloggers. Using internal systems that can find similar malware samples, we were able to then identify another previously unknown sample associated with the attacker. The sample looked like it was developed for testing purposes as opposed to actually being used in attacks. The attacker made a mistake in their operational security with this sample, however, as it included a hardcoded IP address of 95.153.122.210. This IP address was associated with the domain gorkogo77.ddns[.]net, which is also associated with the oyy.name name servers as seen in the diagram below.



The AAAA record for ooy.name also led to a variety of other domains that also had similar IPs and registration information.

Returned 19 RRs in 0.11 seconds.

akb.md.	AAAA	2a01:4f8:120:8355::
www.akb.md.	AAAA	2a01:4f8:120:8355::
static.akb.md.	AAAA	2a01:4f8:120:8355::
akkumulator.md.	AAAA	2a01:4f8:120:8355::
www.akkumulator.md.	AAAA	2a01:4f8:120:8355::
xxhost.ru.	AAAA	2a01:4f8:120:8355::
www.xxhost.ru.	AAAA	2a01:4f8:120:8355::
ddns.su.	AAAA	2a01:4f8:120:8355::
bbxxapp.com.	AAAA	2a01:4f8:120:8355::
www.bbxxapp.com.	AAAA	2a01:4f8:120:8355::
ip2name.com.	AAAA	2a01:4f8:120:8355::
ip2name.net.	AAAA	2a01:4f8:120:8355::
xn--ilaj.net.	AAAA	2a01:4f8:120:8355::
lastmd.org.	AAAA	2a01:4f8:120:8355::
www.lastmd.org.	AAAA	2a01:4f8:120:8355::
oyy.name.	AAAA	2a01:4f8:120:8355::
mail.oyy.name.	AAAA	2a01:4f8:120:8355::
noip.name.	AAAA	2a01:4f8:120:8355::
xn--ilaj.name.	AAAA	2a01:4f8:120:8355::

Looking at the registration information for oyy.name and a number of other domains associated with the above domains, we see the name Igor C***** was used, as well as the common email of “igor.*****@gmail.com” and the phone number “+373.7777*****”. In addition, the addresses were all located in Moldova. While this name may be a pseudonym, we have found it, or variations of it, used consistently across the supporting infrastructure, including on a linked personal social network page.

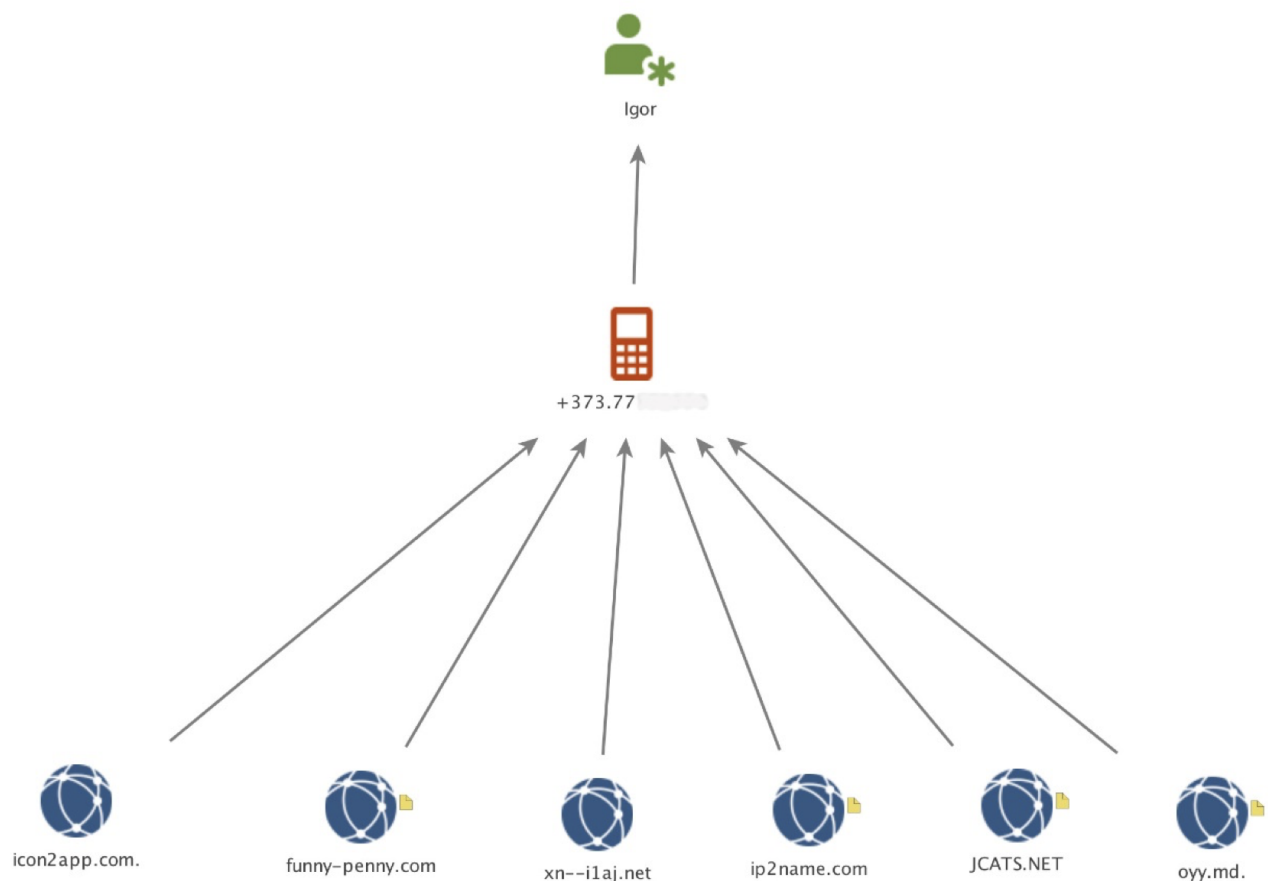
<pre> Domain Name: OYY.NAME Registry Domain ID: 13069216_DOMAIN_NAME-VRSN Registrar WHOIS Server: whois.regtime.net Registrar URL: http://www.webnames.ru Updated Date: 2017-03-15T16:51:04Z Creation Date: 2015-03-29T00:00:00Z Registrar Registration Expiration Date: 2019-03-29T04:00:00Z Registrar: REGTIME LTD. Registrar IANA ID: 1362 Registrar Abuse Contact Email: abuse@regtime.net Registrar Abuse Contact Phone: +7.8463733047 Domain Status: OK Registry Registrant ID: CT1650408-RT Registrant Name: IGOR Registrant Organization: IGOR Registrant Street: str. Kirov 2 Registrant City: Tiraspol Registrant State/Province: MD Registrant Postal Code: 3300 Registrant Country: MD Registrant Phone: +373.77 Registrant Email: support@oyy.name Registry Admin ID: CT1650408-RT </pre>	<pre> Domain Name: LASTMD.ORG Domain ID: D163170153-LROR WHOIS Server: Referral URL: http://www.godaddy.com Updated Date: 2015-11-14T17:48:41Z Creation Date: 2011-08-29T15:03:10Z Registry Expiry Date: 2021-08-29T15:03:10Z Sponsoring Registrar: GoDaddy.com, LLC Sponsoring Registrar IANA ID: 146 Domain Status: clientDeleteProhibited https://icann.org/ Domain Status: clientRenewProhibited https://icann.org/e Domain Status: clientTransferProhibited https://icann.or Domain Status: clientUpdateProhibited https://icann.org/ Registrant ID: CR91232298 Registrant Name: IGOR Registrant Organization: LAST S.R.L. Registrant Street: Karl Liebknecht 333 Registrant City: Tiraspol Registrant State/Province: MD Registrant Postal Code: 3300 Registrant Country: MD Registrant Phone: +373.77 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: igor. @gmail.com Admin ID: CR91232300 Admin Name: IGOR </pre>
--	--


```

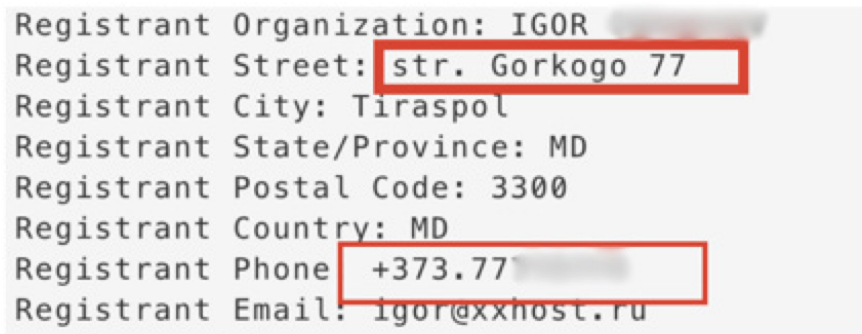
Domain name: oyy.md
Created: 2014-06-08
Expiration date: 2016-06-08
Registrar: OYY SRL
Email: igor. @gmail.com
Name server: ns1.oyy.name 78.46.97.194
Name server: ns2.oyy.name 95.165.150.212

```

Next we looked at the common phone number used and identified a number of domains that were registered with the same registrant phone number, as seen below:



After checking the registration information for each of these domains we identified another tie to the registrant and Bachosens activity. The domain “funny-penny.com”, seen above with the same phone number as related Bachosens domains, used the street address “str. Gorkogo 77”, which matches the previously discovered gorkogo77.ddns.net domain used by Bachosens.



```
Registrant Organization: IGOR [REDACTED]  
Registrant Street: str. Gorkogo 77  
Registrant City: Tiraspol  
Registrant State/Province: MD  
Registrant Postal Code: 3300  
Registrant Country: MD  
Registrant Phone: +373.77 [REDACTED]  
Registrant Email: igor@xxhost.ru
```

Within these related domains, only one appears to have an active business. The domain sells auto parts online.

Furthermore, this online shop actually has a physical shop in Moldova that matches the domain registration information.

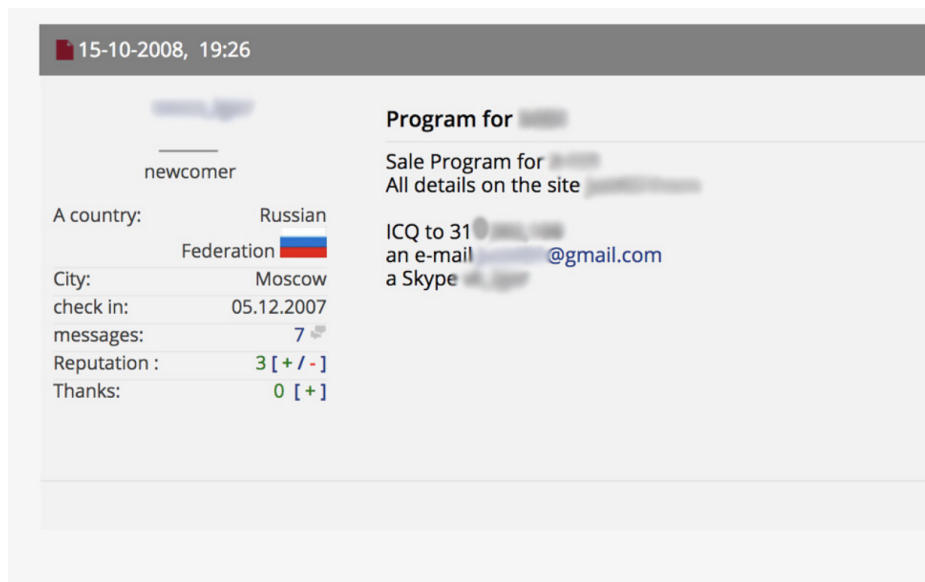
We now knew the registrant of the infrastructure used to compromise an automotive technology supplier was also associated with an automotive parts shop in Moldova. But why this automotive technology supplier was compromised wasn't yet completely clear.

Pivoting off the registration information led to a variety of other sites, including Android applications developed by the same individual and a GitHub site. The aliases and email addresses used on these sites finally led to forum postings with the subjects (translated):

The [DIAG-1000] (All Android / the IOS)

Sale upgrade scan tool [DIAG-1000]

These posts were attempting to sell a stolen version of the exact diagnostic technology produced by the victim automotive supplier. After a lengthy investigation, we discovered the attacker's complex efforts appear to have been simply to steal the technology for resale on the black market—a considerable effort for a technology that can be legitimately purchased for around \$1,100.



“After a lengthy investigation, we discovered the attacker’s complex efforts appear to have been simply to steal the technology for resale on the black market”

Conclusion

Going into this investigation, we thought there was a good chance this would be associated with a nation-state attacker based on the regions of the victims, the highly selective targeting, and the methods in which the malware used covert channels to communicate and go undetected.

The discovery that all of the attacker’s complex coding was for such small financial gain in reselling stolen automotive diagnostic tools was very surprising. The attacks resulted in a meager payout for the attacker, who went through such elaborate means to obtain the automotive diagnostic technology. The legitimate “Diag-1000” is sold new for less than \$1,100 and the stolen version was being sold for \$110.

Based on the Russian strings in the malware infrastructure, Russian characters used for data size suffixes, and the open source traces left by the attacker, we are reasonably confident the attacker is located in Tiraspol, Moldova and is associated with the automotive industry.

This investigation provided us with a good example as to why analysts cannot make assumptions when conducting an investigation and must set a hypothesis, follow the data, and prove or disprove that hypothesis

based on the facts. The initial facts could have led one to believe this was a highly sophisticated operation carried out by a nation state, however, by following the evidence and connecting the dots we were able to develop and see the complete picture of the life cycle of the Bachosens attacks against the victim organizations.

For more information on this investigation, take a look at the Security Response blog on the subject.

Check out the Security Response blog and follow Threat Intel on Twitter to keep up-to-date with the latest happenings in the world of threat intelligence and cybersecurity.

Like this story? Recommend it by hitting the heart button so others on Medium see it, and follow Threat Intel on Medium for more great content.

