+4
4 Votes

Symantec Official Blog

Bachosens: Highly-skilled petty cyber criminal with lofty ambitions targeting large organizations

Eastern Europe based attacker's advanced malware bears comparison with that used by nation-state actors, but basic missteps indicate a threat actor who is skilled but lacking in expertise.

By: **Symantec Security Response (/connect/user/symantec-security-response)** SYMANTEC EMPLOYEE

Created 31 May 2017 0 Comments : 简体中文 (/connect/zh-hans/blogs/bachosens)

0 14

(http://en-us.reddit.com/submit?url=http://www.symantec.com/connect/blogs/bachosens-highly-skilled-petty-cyber-criminal-lofty-ambitions-targeting-large-organizations)
(/connect/forward?path=node/3685521)
Like 0

In attacks reminiscent of the early days of malware, a lone wolf threat actor who appears to be based in a disputed part of eastern Moldova is using advanced malware to carry out cyber attacks against large organizations for relatively modest rewards. The malware in question, Trojan.Bachosens (https://www.symantec.com/security_response/writeup.jsp?docid=2017-022316-1436-99), was so advanced that Symantec analysts initially thought they were looking at the work of nation-state actors. However, further investigation revealed a 2017 equivalent of the hobbyist hackers of the 1990s—the only difference being this hacker wasn't out for bragging rights. He was out for financial reward.

Big weapon, small rewards

This lone wolf attacker—who we call Igor—is not an average cyber criminal with the aim of infecting as many victims as possible. Rather, he has been carrying out highly targeted attacks on specific organizations.

Igor developed a specialized tool, a piece of malware called Bachosens, to gain access to at least two large organizations, an international airline and a Chinese auto-tech company. Symantec believes that Igor planted the malware through the use of spear-phishing emails, a tactic typically employed by nation-state actors.

Igor targeted the auto-tech company in order to steal car diagnostics software. This software retails for approximately $1,100 through legitimate channels. Igor is selling it for just a few hundred dollars on underground forums and websites he has created expressly for this purpose. Considering the audacity of this attack, the financial rewards for Igor are pretty low.

There are indications that Igor has been active for quite some time. Symantec first identified the use of Bachosens in 2014. However, the auto-tech company targeted by Igor issued an alert as far back as 2009 about its software being sold by an unauthorized reseller. Symantec was able to confirm links between the domains mentioned in this alert and Igor, indicating he has been active for almost 10 years.

2009	Chinese auto-tech company issues alert about unauthorized sellers of its software. Domains mentioned in alert linked to Igor.
2013	Variant of keylogger first spotted.
2014	Bachosens malware first seen in submission to Virus Total.
February 2016	Earliest Bachosens infection seen in the wild.
April 2016	Phishing email containing Bachosens malware sent to online gambling company.

September 2016	Bachosens malware found on airline systems.

Figure 1. Timeline showing Igor has been active for almost 10 years

Symantec researchers' analysis of Igor's activities allowed us to gain an insight into his methods and areas of focus. Based on publicly available information, Symantec was able to find likely connections between Igor and an auto parts store located in Transnistria, a disputed territory in Moldova. His involvement in the automotive industry could explain why he showed an interest in targeting the auto-tech company.

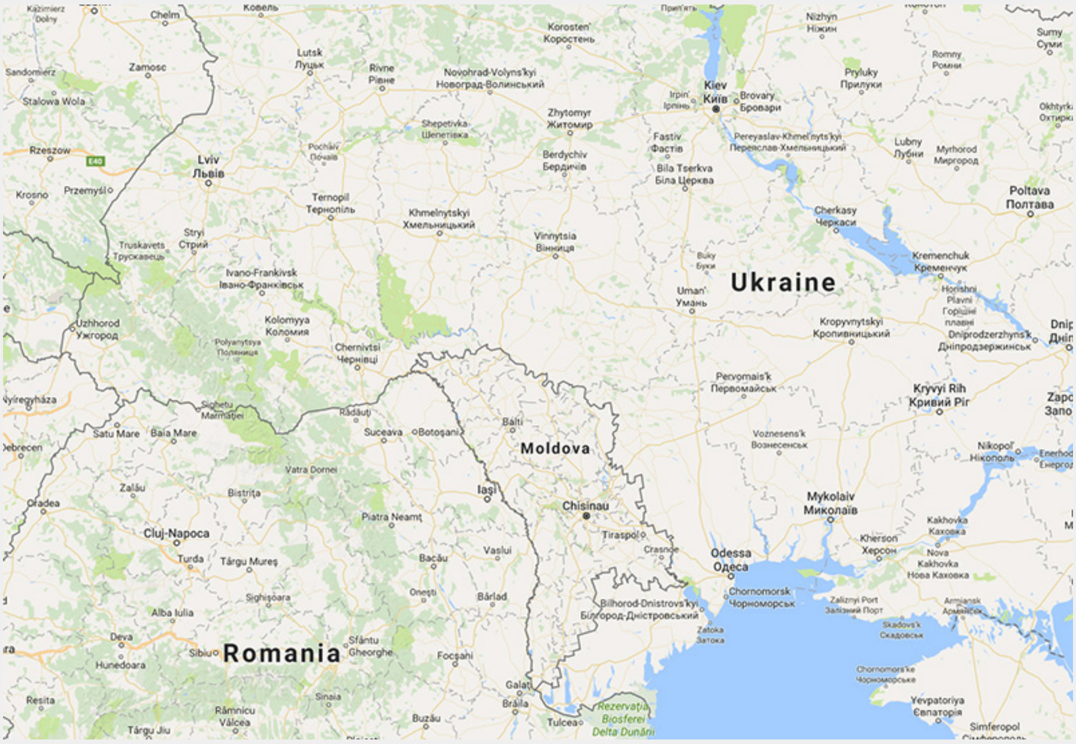


Figure 2. The disputed republic of Transnistria, and its capital Tiraspol, is located in eastern Moldova, on the border with Ukraine

While the targeting of the Chinese auto-tech company with this malware seems to have an obvious aim—to steal software with the aim of selling it and making money—Symantec also saw some activity that is harder to explain.

The Bachosens Trojan was also found on a number of systems in a large commercial airline, however, the motive for this attack is unclear at this time. Symantec is confident that this malware is only being used by Igor. Our evidence also shows that Igor's campaigns are highly targeted, therefore it's unlikely that this infection was accidental.

There is also evidence Igor attempted to infect an online gambling organization. He used targeted spear-phishing emails with an attachment containing malicious macros in this infection attempt, which was ultimately unsuccessful.

This is an attacker who is made up of contradictions: he uses well-developed malware, but makes some basic operational mistakes that allowed Symantec researchers to uncover a lot about his activities.

Highly-skilled petty cyber criminal is using advanced malware to target large organizations for meager gain #infosec

CLICK TO TWEET (HTTPS://TWITTER.COM/INTENT/TWEET?TEXT=HIGHLY-SKILLED+PETTY+CYBER+CRIMINAL+IS+USING+ADVANCED+MALWARE+TO+TARGET+LARGE+ORGANIZATIONS+FOR+MEAGER+GAIN+%23INFOSEC&SO HIGHLY-SKILLED-PETTY-CYBER-CRIMINAL-LOFTY-AMBITIONS-TARGETING-LARGE-ORGANIZATIONS&VIA=THREATINTEL&RELATED=SYMANTEC)

High-level malware, low-level mistakes

As previously mentioned, this malware is highly sophisticated, displaying a technical competency similar to that seen in malware used by nation-state actors, indicating that its developer has a high level of skill.

It is possible Igor purchased this malware from another developer, however, as no one else has been observed online using it, Symantec researchers believe this is unlikely, and believe that Igor developed this malware himself.

Elements of this attack that make it stand out from the ordinary include the use of rarely used covert communication channels, such as DNS, ICMP, and HTTP, to communicate with the command and control (C&C) server. The attacker also encrypts the victim's information before it is transmitted to the C&C server, with the malware programmed to create a set of ephemeral AES keys to encrypt the data before sending it.

He also sends these communications over IPv6, which can make them harder to detect than if sent over IPv4.

Igor also uses dynamic DNS (DDNS) and domain generation algorithms (DGA). DGA is used to generate a prefix, which is added to a DDNS controlled root domain to form the C&C server.

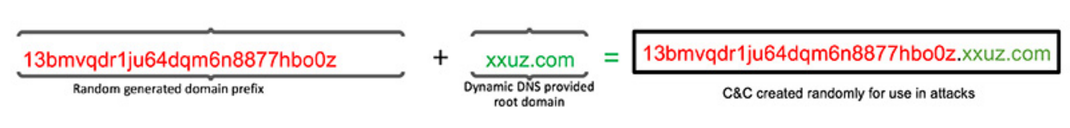
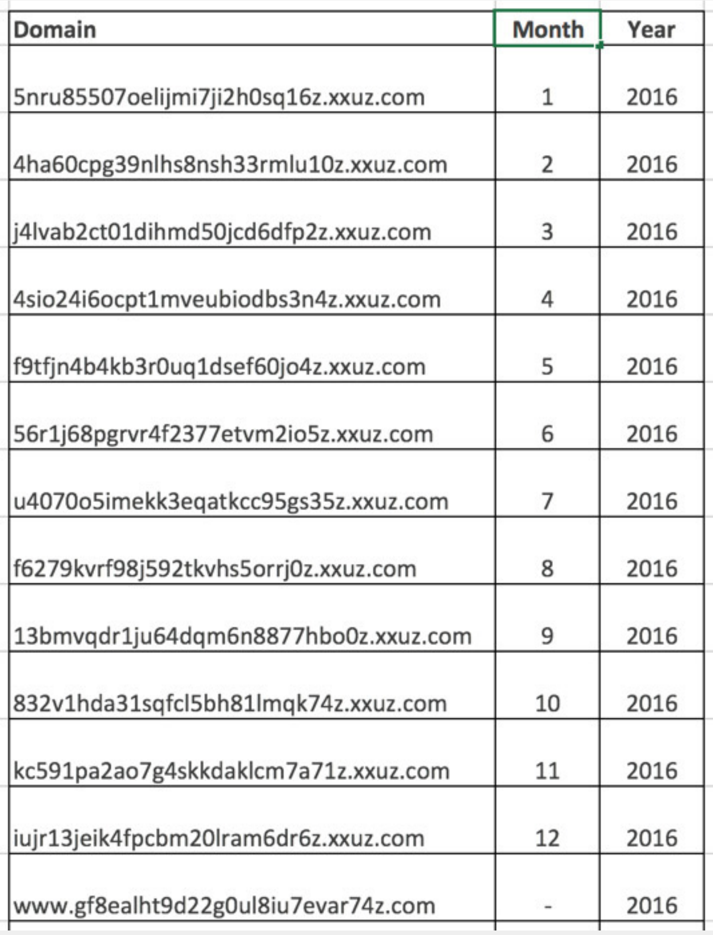

13bmvqdr1ju64dqm6n8877hbo0z
Random generated domain prefix
+
xxuz.com
Dynamic DNS provided root domain
=
13bmvqdr1ju64dqm6n8877hbo0z.xxuz.com
C&C created randomly for use in attacks

Figure 3. How the C&C is created

Oddly, while malware that uses DGA normally creates hundreds of domains at a time—with the aim being to make it more difficult for the malware to be detected—this attacker only created 13 domains using DGA over the course of an entire year. One domain was valid for the entire year, with one new domain created each month. Creating such a small number of domains essentially defeats the purpose of using DGA, as it would only allow the attacker to avoid the most basic cyber defenses.

This unusual use of DGA is just one of the parts of Igor's operations that demonstrates a lack of polish, and shows an interesting contradiction between the advanced level of the malware and the rather unpolished way in which it is used.



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
56r1j68pgrvr4f2377etvm2io5z.xxuz.com	6	2016
u4070o5imekk3eqatkcc95gs35z.xxuz.com	7	2016
f6279kvrf98j592tkvhs5orrj0z.xxuz.com	8	2016
13bmvqdr1ju64dqm6n8877hbo0z.xxuz.com	9	2016
832v1hda31sqfcl5bh81lmqk74z.xxuz.com	10	2016
kc591pa2ao7g4skkdaklcm7a71z.xxuz.com	11	2016
iujr13jeik4fpcbm20lram6dr6z.xxuz.com	12	2016
www.gf8ealht9d22g0ul8iu7evar74z.com	-	2016

Figure 4. The 13 domains used by the attacker in 2016

Igor submitted malware samples to Virus Total to test the detection capabilities of defenders, and used development names (such as mod_exe and mod_dll) in the submission, which would draw attention to it. It is known that malicious hackers often use Virus Total, a tool that analyzes URLs and files to detect malware, to test the malware they are developing. Using development file names indicates that a piece of malware is a work in progress and is more likely to draw the attention of investigators.

The malware was also found packaged with computer games, which is not generally something that would be seen in advanced attacks. In fact, Symantec researchers first realized that this malware was unlikely to be the work of a nation state or sophisticated cyber attacker when they found it packaged with an online video game.

Igor also used an unobfuscated keylogger, something professional cyber attackers are very unlikely to do. He also posted personal information on publicly accessible auto forums where he was attempting to sell the stolen software, exposing himself as a likely perpetrator.

These various missteps indicate that while Igor may be talented enough to create highly advanced malware, he lacks the expertise of more professional cyber attackers.

Petty #cyber criminal's advanced #malware bears comparison with tools used by nation-state actors

CLICK TO TWEET (HTTPS://TWITTER.COM/INTENT/TWEET?TEXT=PETTY+%23CYBER+CRIMINAL%27S+ADVANCED+%23MALWARE+BEARS+COMPARISON+WITH+TOOLS+USED+BY+NATION-STATE+ACTORS&SOURCE=THREATINTEL&URL=HTTP%3A%2F%2FWWW.SYMANTEC.COM%2FCONNECT%2FBLOGS%2FBACHOSENS-HIGHLY-SKILLED-PETTY-CYBER-CRIMINAL-LOFTY-AMBITIONS-TARGETING-LARGE-ORGANIZATIONS&VIA=THREATINTEL&RELATED=SYMANTEC)

What do we know about this attacker?

Symantec researchers' investigations have turned up quite a lot of information about this cyber attacker.

Symantec believes he may be based in the town of Tiraspol in eastern Moldova. Officially, Tiraspol is the second-largest city in Moldova, but it is also the capital of the self-declared republic of Transnistria, which is not recognized as an independent state by the UN.

The dominant language in Transnistria is Russian, and there were Russian strings used in the Bachosens malware, and communication with the C&C server uses what appears to be the Russian equivalents of size suffixes for KB, MB, GB, and TB. This had indicated to researchers that the individual behind this malware was likely Russian speaking.

The level of information the attacker knowingly or negligently revealed about himself online gave us high confidence that he is an individual involved in the auto industry who is based in this part of Eastern Europe.

His likely location in Tiraspol may also explain why he appears to have such modest aims when it comes to the gains he seems to be making from cyber crime. Although it is hard to get official data given it is a disputed territory, the average monthly salary in Transnistria has been reported as being as little as a few hundred euro. In that context, selling stolen software online for a few hundred euro could represent quite the windfall for an individual based in that part of the world.

Petty cyber crime still exists

While we have gleaned a lot of information about this attack, much of this attacker's activity remains a mystery, such as the motivations behind some of his activity, and where he may have acquired the skills to create such sophisticated malware, while clearly demonstrating lack of expertise in other areas.

However, this activity does show us that while nation-state actors and organized cyber crime gangs carrying off big heists may be what grabs headlines, there are still lone wolf attackers out there making a comfortable living from cyber crime.

Protection

Symantec and Norton products have the following detections in place for the threats called out in this blog:

- Trojan.Bachosens (https://www.symantec.com/security_response/writeup.jsp?docid=2017-022316-1436-99)

For a technical analysis of the details of this investigation, please read our analyst's blog on Medium (https://medium.com/threat-intel/cybercrime-investigation-insights-bachosens-e1d6312f6b3a).

Tags: Security Response (/connect/search?filters=im_vid_51:2261), AIT (/connect/search?filters=im_vid_111:102921), Bachosens (/connect/search?filters=im_vid_111:105231), cyber crime (/connect/search?filters=im_vid_111:47041), cyber criminal (/connect/search?filters=im_vid_111:58001), Europe (/connect/search?filters=im_vid_111:105221), Malware (/connect/search?filters=im_vid_111:8691)

Subscriptions (0)

(/connect/user/symantec-security-response)

Symantec Security Response (/connect/user/symantec-security-response)

View Profile (/connect/user/symantec-security-response)

Login (/connect/user/login?destination=node%2F3685521) or Register (/connect/user/register?destination=node%2F3685521) to post comments.