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

medium.com/threat-intel/cybercrime-investigation-insights-bachosens-e1d6312f6b3a

Jon DiMaggio

April 3, 2018

Jon DiMaggio

May 31, 2017

·

10 min read

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.

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%

%System%

%System%

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.

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:

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, "lok4723peoi8n1c0mk23rtmc91z" is decrypted to "0c23ca440908c1e8030102000000000", which can be decoded into the "infection id" and infection date below:

nonce = 0c

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 DNS 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, б and гб 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 oyy.name also led to a variety of other domains that also had similar IPs and registration information.

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.

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.

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.

Check out the Security Response and follow Threat Intel on 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.