Endpoint Protection

community.broadcom.com/symantecenterprise/viewdocument/iran-based-attackers-use-back-door

Dec 07, 2015 08:59 AM

A L Johnson

Two teams of Iran-based attackers have been using back door threats to conduct targeted surveillance of domestic and international targets. While the groups are heavily targeting individuals located in Iran, they've also compromised airlines and telecom providers in the Middle East region, possibly in an attempt to monitor targets' movements and communications.

The attackers are part of two separate groups that have a shared interest in targets. One group, which we call Cadelle, uses Backdoor.Cadelspy, while the other, which we've named Chafer, uses Backdoor.Remexi and Backdoor.Remexi.B. These threats are capable of opening a back door and stealing information from victims' computers

The Cadelle and Chafer groups

Symantec telemetry identified Cadelle and Chafer activity dating from as far back as July 2014, however, it's likely that activity began well before this date. Command-and-control

(C&C) registrant information points to activity possibly as early as 2011, while executable compilation times suggest early 2012. Their attacks continue to the present day. Symantec estimates that each team is made up of between 5 and 10 people.

The back door threats that the groups use appear to be custom made. It's unclear how Cadelle infects its targets with Backdoor.Cadelspy. However, Chafer has been observed compromising web servers, likely through SQL injection attacks, to drop Backdoor.Remexi onto victims' computers. Chafer then uses Remexi to gather user names and passwords to help it spread further across the network.

There is evidence to suggest that the two teams may be connected in some way, though we cannot confirm this. A number of computers experienced both Cadelspy and Remexi infections within a small time window. In one instance, a computer was compromised with Backdoor.Cadelspy just minutes after being infected with Backdoor.Remexi. The Cadelle and Chafer groups also keep the same working hours and focus on similar targets. However, no sharing of C&C infrastructure between the teams has been observed.

If Cadelle and Chafer are not directly linked, then they may be separately working for a single entity. Their victim profile may be of interest to a nation state.

The victims

Data from Cadelle's C&C servers shows that a large number of Backdoor.Cadelspy infections affected individual users of Iranian internet service providers (ISPs) and hosting services. This suggests that the majority of victims are based in Iran. There was also a significant amount of individual targets that used anonymous proxy services to go online. Reports have shown that many Iranians avail of these services to access sites that are blocked by the government's internet censorship measures. Dissidents, activists, and researchers in the region may use these proxies in an attempt to keep their online activities private.

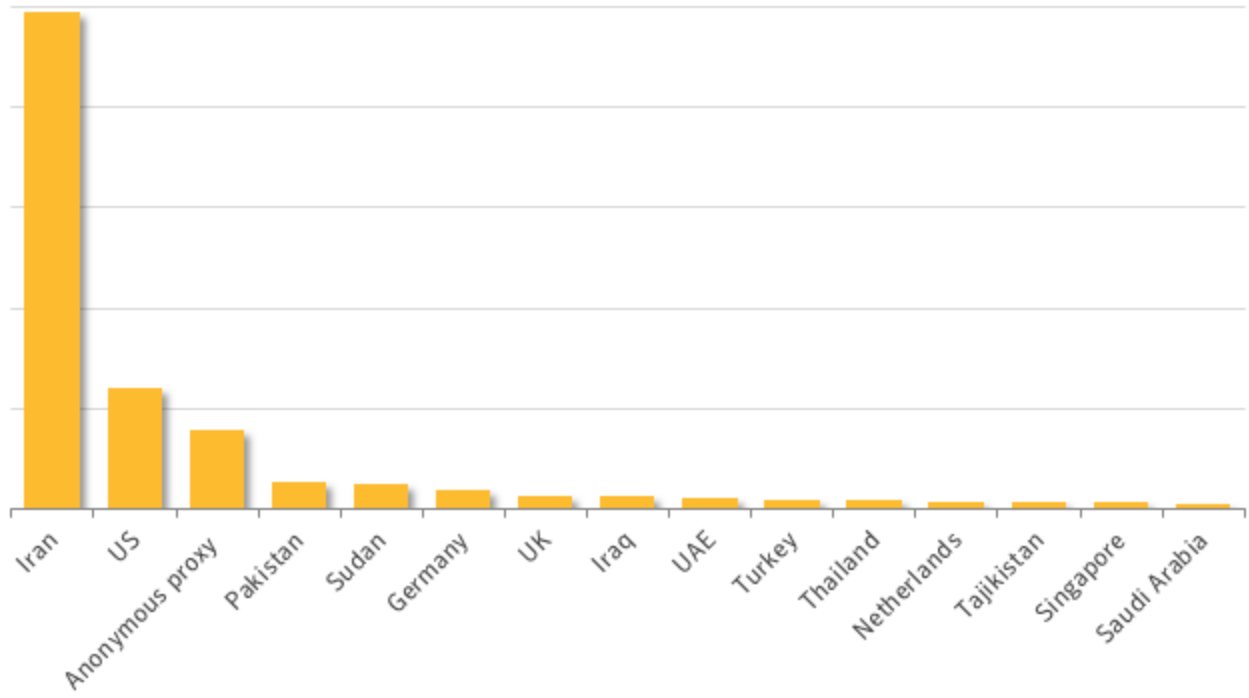

Figure 1. Backdoor.Cadelspy infections by region

In terms of targeted organizations, both Cadelle and Chafer seem to be interested in a similar category of organizations, such as airlines and telecom companies. The affected organizations we were able to identify are mostly based in the Middle East region in countries such as Saudi Arabia and Afghanistan, while one organization is located in the US.

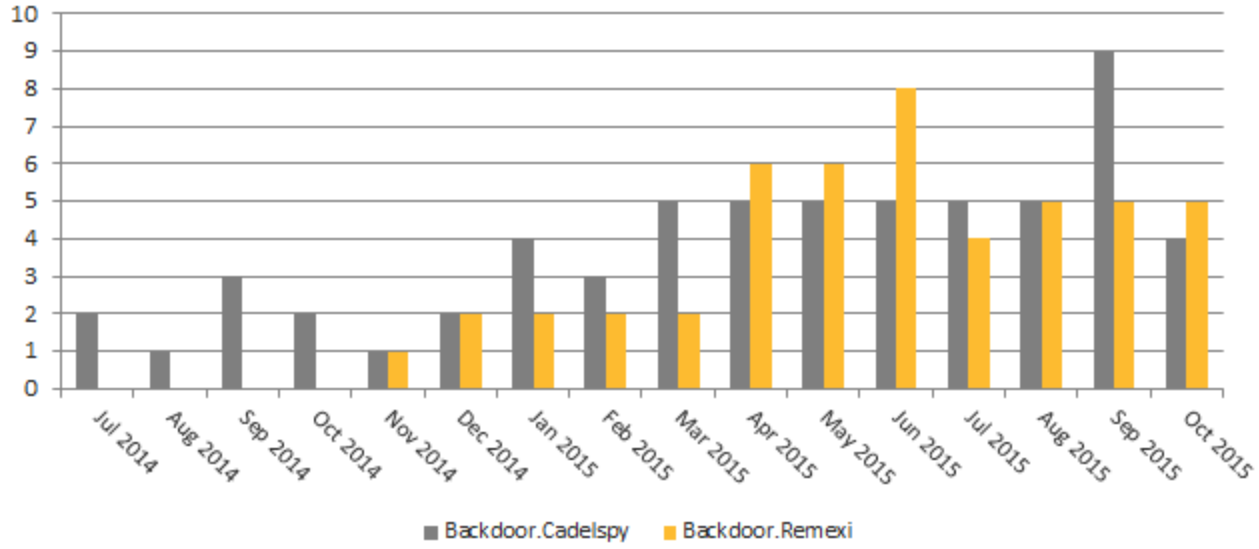

Figure 2. Number of unique organizations hit with Backdoor.Cadelspy and Backdoor.Remexi from July 2014 to October 2015

Our telemetry shows that among more than a dozen entities that experienced Cadelspy and Remexi infections, four of them were compromised with both of the threats at some stages. In most instances, victim computers were infected with either Backdoor.Cadelspy or Backdoor.Remexi, not both. Less than five percent of computers were infected with both malware families. In one affected organization, there was intermittent activity between the threats over ten months. A combined total of 60 computers were compromised in another organization for almost a year.

The malware's activity on victim computers appears to depend on the targets. One computer that was infected with both Cadelspy and Remexi was a system that ran a SIM card editing application. Other compromised computers included those belonging to web developers, or are file and database servers.

The nature of the victims suggests that Cadelle and Chafer are primarily interested in tracking individuals in terms of their movements and communications. Compromising regional telcos and airlines can help the attackers achieve this aim.

Based in Iran?

There are a number of factors in these groups' campaigns that suggests that the attackers may be based in Iran. Cadelle and Chafer are most active during the day time within Iran's time zone and primarily operate during Iran's business week (Saturday through Thursday).

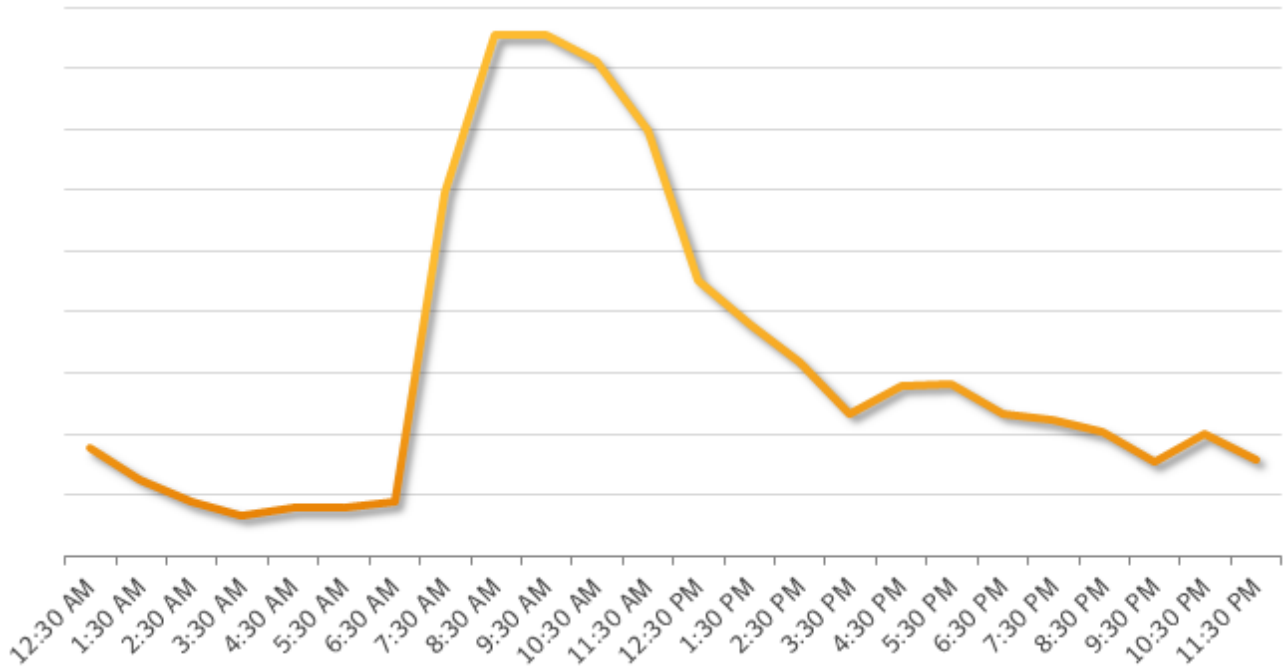

Figure 3. Cadelle and Chafer's activity levels by hour in Iran's time zone (UTC +3.5)

Additionally, Symantec observed that Backdoor.Cadelspy's file strings seem to include dates written in the Solar Hijri calendar, which is used in Iran and Afghanistan. While the Gregorian calendar marks the current year as 2015, the Solar Hijri calendar states that it is 1394. When we converted the dates in the file strings from the Solar Hijri calendar to the Gregorian one, we found that they were close to the compilation times of the executables and also close to when Cadelle's targets were initially compromised.

Based on our analysis, we believe that Cadelle and Chafer's victims are most likely to be of interest to an Iranian entity. Cadelle and Chafer are by no means the first Iran-based attack group to appear. Other groups attributed to Iranian attackers, such as Rocket Kitten, have targeted Iranian individuals in the past, including anonymous proxy users, researchers, journalists, and dissidents. Backdoor.Remexi activity in particular is reminiscent of Operation Cleaver, as documented by Cylance, and may possibly be a continuation of that activity.

Cadelle and Chafer's malware

The groups use one malware family each to open a back door and steal information from the compromised computer. Cadelle uses Backdoor.Cadelspy while Chafer operates with Backdoor.Remexi and Backdoor.Remexi.B.

Cadelspy initially arrives on the computer as a dropper, which downloads two installer components catering to whether the victim is running a 32-bit or 64-bit system. The dropper then executes the appropriate installer, which launches Cadelspy's malicious payload and allows it to run whenever any Windows program is executed.

Cadelspy's main payload contains its back door functionality, allowing the threat to carry out the following activities:

- Log keystrokes and the titles of open windows
- Gather clipboard data and system information
- Steal printer information and any documents that were sent to be printed
- Record audio
- Capture screenshots and webcam photos

Cadelspy compresses all of the stolen data into a .cab file and uploads it to the attacker's C&C servers. The threat is also able to update its configuration file to gain additional features.

Meanwhile, Chafer's threat Remexi contains fewer features than Cadelle's Cadelspy does. Remexi is a basic back door Trojan that allows attackers to open a remote shell on the computer and execute commands. Though this is unsophisticated, a remote shell does provide a highly flexible and powerful means of remote access in the hands of a skilled attacker.

Mitigation

Cadelle and Chafer's activities show that attack groups don't need advanced skills to conduct effective targeted espionage against victims. The two groups' threats have managed to remain on their targets' computers for almost a year, potentially giving the attackers access to an enormous amount of sensitive information. They're also aware that they don't only have to directly attack the individuals, as they can get to their victims by compromising the services that they use, such as airlines and telcos.

Both Cadelle and Chafer are still active today and we don't expect to see them end their activities any time soon. Individuals and organizations wishing to avoid being compromised by these teams should adhere to the following advice:

- Ensure that software on computers and servers is being regularly updated to prevent known vulnerabilities from being exploited
- Treat unsolicited emails with suspicion. Targeted attacks frequently distribute malware through malicious links and attachments in emails.
- Keep security software up-to-date with the latest definitions

Protection

Norton Security, Symantec Endpoint Protection, and other Symantec security products protect users against these threats through the following detections:

AV

IPS

Indicators of compromise

We have also compiled an indicators-of-compromise document containing further details which can be used to help identify the threats if they are present in your environment.