The Great Bank Robbery: the Carbanak APT

By GReAT

Published: 2015-02-16 · Archived: 2026-04-05 16:32:03 UTC

Download Full Report PDF

The story of Carbanak began when a bank from Ukraine asked us to help with a forensic investigation. Money was being mysteriously stolen from ATMs. Our initial thoughts tended towards the Tyupkin malware. However, upon investigating the hard disk of the ATM system we couldn't find anything except a rather odd VPN configuration (the netmask was set to 172.0.0.0).

At this time we regarded it as just another malware attack. Little did we know then that a few months later one of our colleagues would receive a call at 3 a.m. in the middle of the night. On the phone was an account manager, asking us to call a certain number as matter of urgency. The person at the end of the line was the CSO of a Russian bank. One of their systems was alerting that data was being sent from their Domain Controller to the People's Republic of China.

> Up to 100 financial institutions have been hit.Total financial losses could be as a high as $1bn#TheSAS2015#Carbanak
>
> Tweet

When we arrived on site we were quickly able to find the malware on the system. We wrote a batch script that removed the malware from an infected PC, and ran this script on all the computers at the bank. This was done multiple times until we were sure that all the machines were clean. Of course, samples were saved and through them we encountered the Carbanak malware for the first time.

Modus Operandi

Further forensic analysis took us to the point of initial infection: a spear phishing e-mail with a CPL attachment; although in other cases Word documents exploiting known vulnerabilities were used. After executing the shellcode, a backdoor based on Carberp, is installed on the system. This backdoor is what we know today as Carbanak. It is designed for espionage, data exfiltration and remote control.

> Each bank robbery took 2-4 months, from infecting the first computer to cashing the money out #TheSAS2015 #Carbanak
>
> Tweet

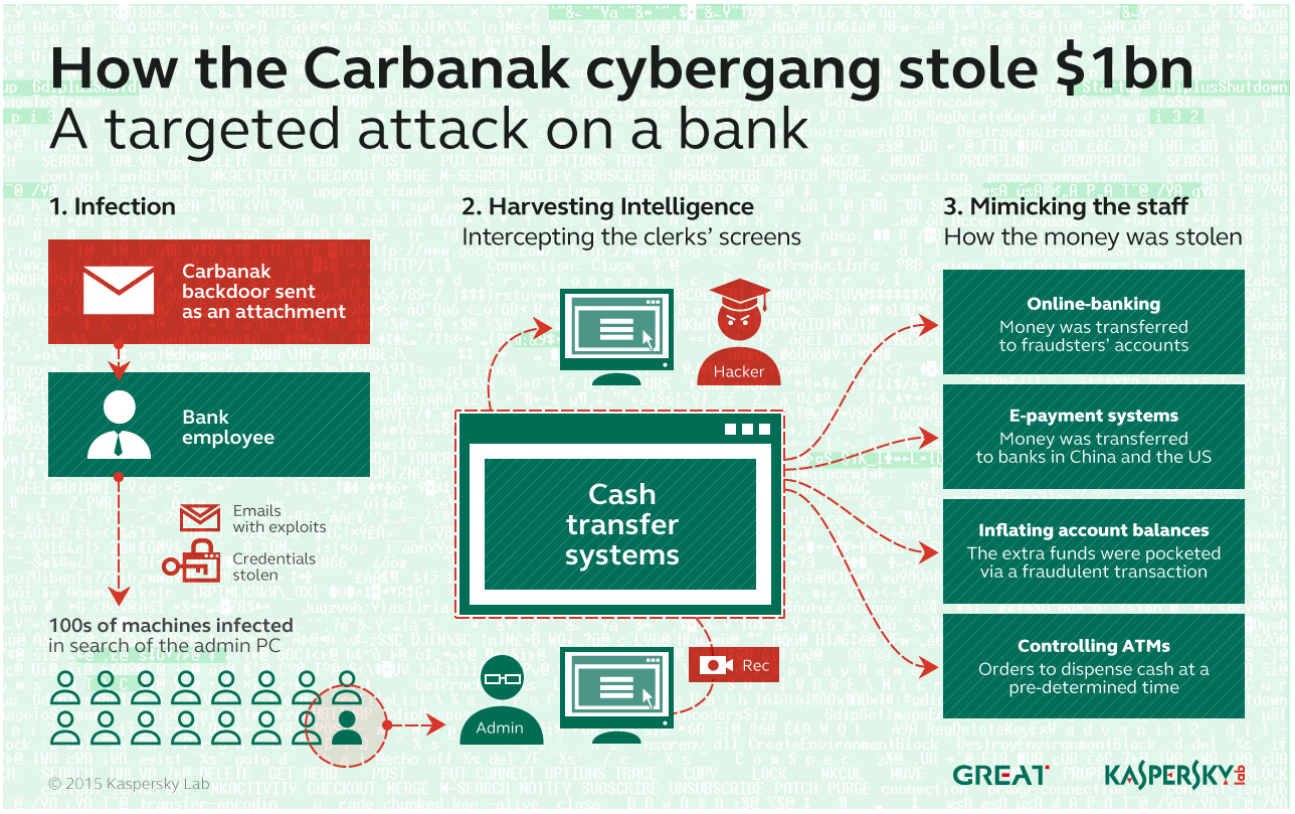
Once the attackers are inside the victim´s network, they perform a manual reconnaissance, trying to compromise relevant computers (such as those of administrators') and use lateral movement tools. In short, having gained access, they will jump through the network until they find their point of interest. What this point of interest is, varies according to the attack. What they all have in common, however, is that from this point it is possible to extract money from the infected entity.

The gang behind Carbanak does not necessarily have prior knowledge of the inner workings of each bank targeted, since these vary per organisation. So in order to understand how a particular bank operates, infected computers were used to record videos that were then sent to the Command and Control servers. Even though the quality of the videos was relatively poor, they were still good enough for the attackers, armed also with the keylogged data for that particular machine to understand what the victim was doing. This provided them with the knowledge they needed to cash out the money.

Cash out procedures

During our investigation we found several ways of cashing out:

ATMs were instructed remotely to dispense cash without any interaction with the ATM itself, with the cash then collected by mules; the SWIFT network was used to transfer money out of the organisation and into criminals' accounts; and databases with account information were altered so that fake accounts could be created with a relatively high balance, with mule services being used to collect the money.



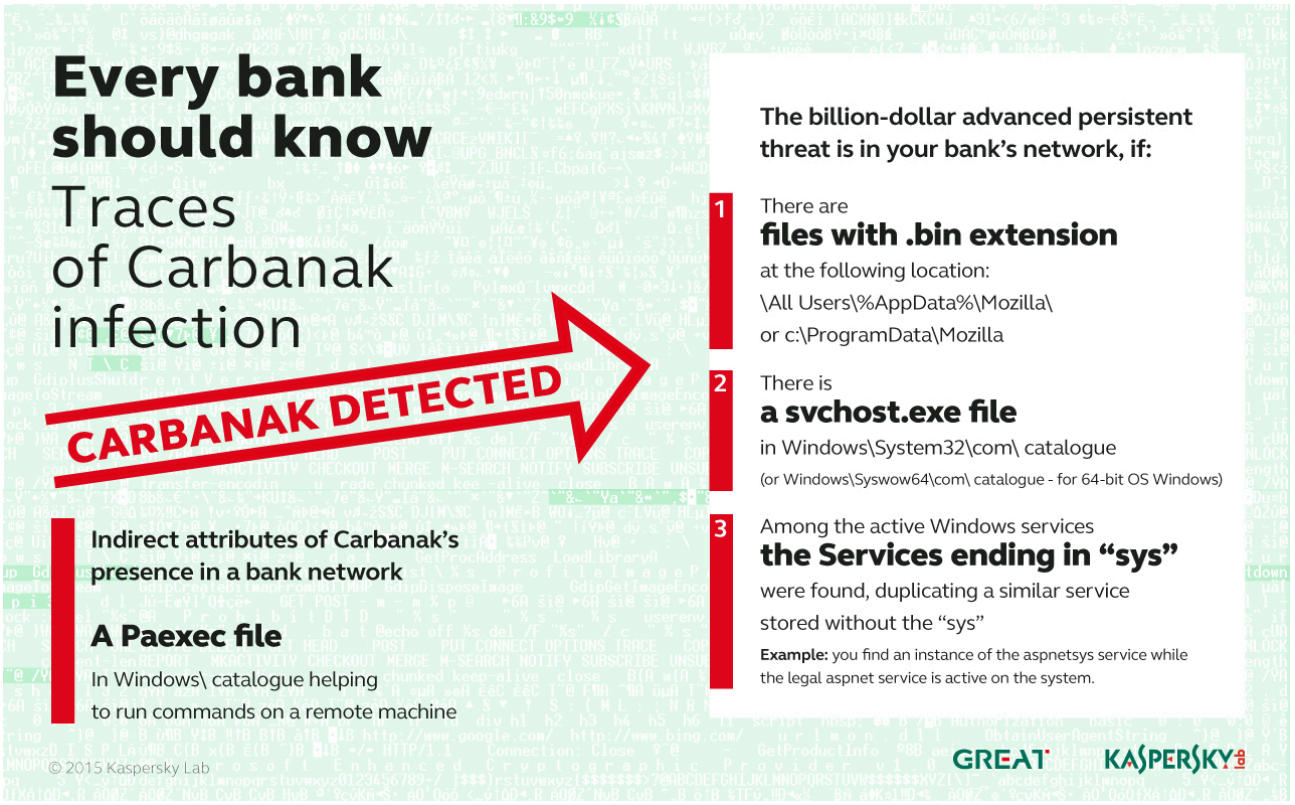
Infections and losses

Since we started investigating this campaign we have worked very closely with the law enforcement agencies (LEAs) tracking the Carbanak group. As a result of this cooperation we know that up to 100 targets have been hit. When it comes to financial institutions, In at least half of the cases the criminals were able to extract money from the infected institution. Losses per bank range from $2.5 million to approximately $10 million. However, according to information provided by LEAs and the victims themselves, total financial losses could be as a high as $1 billion, making this by far the most successful criminal cyber campaign we have ever seen.

> Losses from #Carbanak per bank range from $2.5 million to approximately $10 million #TheSAS2015
>
> Tweet

Our investigation began in Ukraine and then moved to Moscow, with most of the financial entities targeted by the group located in Eastern Europe. However thanks to KSN data and data obtained from the Command and Control servers, we know that Carbanak also targets victims in the USA, Germany and China. Now the group is expanding its operations to new areas. These include Malaysia, Nepal, Kuwait and several regions in Africa, among others.

The group is still active, and we urge all financial organizations to carefully scan their networks for the presence of Carbanak. If detected, report the intrusion to law enforcement immediately.



For a full description of the campaign, IOCs and list of infections please see our report.

To check your network for Carbanak's presence, you can also use the open IOC file available here.

FAQ

What is Carbanak?

Carbanak is the name we use for an APT-style campaign targeting (but not limited to) financial institutions. The main difference with other APT attacks is that attackers do not see data but money as their primary target. We say APT-like, however the attack is not strictly speaking Advanced. Strictly speaking, the main feature defining the attackers is Persistence.

We name the backdoor Carbanak since it is based on Carberp and the name of the configuration file is "anak.cfg".

What are the malicious purposes of this campaign?

The attackers infiltrate the victim´s network looking for the critical system they can use for cashing money out. Once they have stolen a significant amount of money (from 2.5 to 10 MM USD per entity), they abandon the victim.

Why do you think it is significant?

Banking entities have always been a primary target for cybercriminals. However it was almost always through their customers. This time attackers are targeting financial entities directly in an unprecedented, determined,

highly professional and coordinated attack, and using any means from the target to cash as much money out as possible, up to an apparently auto-imposed limit.

Can you explain the timeline of the campaign?

According to what we know, the first malicious samples were compiled in August, 2013 when the cybercriminals started to test the Carbanak malware. The first infections were detected in December, 2013.

On average, each bank robbery took between two and four months, from infecting the first computer at the bank's corporate network to cashing the money out.

We believe that the gang was able to successfully steal from their first victims during the period of February-April 2014. The peak of infections was recorded in June 2014.

Currently the campaign is still active.

Why didn´t you make the details public until now?

Since we started working on this campaign we have collaborated with the different LEAs involved in the investigation and helped them as much as possible. As it remains an open investigation, we were asked not to share any details until it was safe to do so.

Have you reached victims and Computer Emergency Response Teams (CERTs) in those countries where you have detected the incidents?

Yes, this investigation turned into a joint operation between Kaspersky Lab's Global Research and Analysis Team and international organizations, national and regional law enforcement agencies and a number of Computer Emergency Response Teams (CERTs) worldwide.

One of our main goals was to disseminate our knowledge of the campaign and IOCs among all detected and potential victims. We used national CERTs and LEAs as the distribution channel.

How did you contribute to the investigation?

We're helping to assist in investigations and countermeasures that disrupt malware operations and cybercriminal activity. During the investigations we provide technical expertise such as analyzing infection vectors, malicious programs, supported Command & Control infrastructure and exploitation methods.

How was the malware distributed?

Attackers used spear phishing emails with malicious attachments against employees of the targeted financial institutions, in some cases sending them to their personal email addresses. We believe the attackers also used drive by download attacks, but this second assumption is still not 100% confirmed.

What is the potential impact for victims?

Based on what the attackers stole from victims, a new victim faces potential losses of up to 10 million $. However this figure is arbitrary based on what we know: nothing limits the potential loss once an institution is infected.

Who are the victims? What is the scale of the attack?

Victims are mainly institutions in the financial industry; however we have also found traces of infections in POS terminals and PR agencies. For a sense of the scale of the attack please see the different charts and maps we provide in our report.

As with many malware campaigns there are a variety of companies/individuals analyzing the malware, resulting in requests to the Command and Control server. When we analyze those servers, all we see are the IPs and possibly some additional information. When this additional information is not present, and when the IP cannot be traced back to its owner, we mark it as an infection.

Based on this approach our analysis concludes that Russia, the US, Germany and China are the most affected countries in number of traces of infection (IP addresses).

How are corporate users protected against this type of attack? Does Kaspersky Lab protect their users?

Yes, we detect Carbanak samples as Backdoor.Win32.Carbanak and Backdoor.Win32.CarbanakCmd.

All Kaspersky Lab's corporate products and solutions detect known Carbanak samples. To raise the level of protection, it is recommended to switch on Kaspersky's Proactive Defense Module included in each modern product and solution.

We also have some general recommendations:

- Do not open suspicious emails, especially if they have an attachment;
- Update your software (in this campaign no 0days were used);
- Turn on heuristics in your security suites, this way it is more likely that such new samples will be detected and stopped from the beginning.