ALERT: Point of Sale RAM scraper malware

Advances in technology have led to more sophisticated crimes by exploiting security vulnerabilities of new technologies. This is exacerbated by the fact that understanding of these technologies and their use is only by a few, while the majority of end-users are unaware. Generally speaking, following standard security practices will thwart 95% of electronic crimes such as phishing, hacking, etc. This includes using complex passwords (Sf9$fpq%f82bsS), using network firewalls, encrypted emails, etc. But the new POS RAM scraper is dangerous because the vendors are not the victims of their bad security, and you may never know where your credit card or other information was scraped from.

A look at Point of Sale RAM scraper malware and how it works

From Sophos:

A special kind of malware has been hitting the headlines recently – that which attacks the RAM of Point of Sale (PoS) systems.

Although it's been getting quite a bit of publicity recently, we actually first identified it as a threat back in December 2009 and wrote about it in an article on Naked Security entitled Will RAM scraping loosen the sky and make it fall?.

Answering that question today, it just might!

Actually, the situation isn't that bad – yet – but this malware family has definitely become more complex and far-reaching. In this article, we take a step back from the technical details and look at the evolution of PoS RAM scrapers.

What do PoS RAM scrapers do?

In a nutshell, PoS RAM scrapers steal payment data – such as credit card track one and track two data – from the RAM of PoS systems.

The payment card industry has a set of data security standards known asPCI-DSS. These standards require end-to-end encryption of sensitive payment data when it is transmitted, received or stored.

This payment data is decrypted in the PoS's RAM for processing, and the RAM is where the scraper strikes. Using regular expression searches, they harvest the clear-text payment data and send that information to rogue callhome servers.

Why do we care about PoS RAM scrapers? How does it hurt me?

I believe this malware family has a higher probability of burning a hole in your pocket compared to other prevalent malware families.

In today's plastic money economy people are carrying cash a lot less than before. Aside from a handful of stores, the majority of retailers accept debit or credit cards. Payment cards are convenient, quick, supposedly-secure, and you don't have change jingling around in your pockets.

PoS RAM scrapers target the systems which process debit and credit card transactions and steal the sensitive payment information. Your home computer might be super secure, but

there is no guarantee the PoS system at your neighborhood grocery store has the same level of security. You might end up losing your credit card data buying a candy bar!

How have PoS RAM scrapers evolved?

Sophos detects PoS RAM scraper malware under the family name *Trackr*(e.g. Troj/Trackr-Gen, Troj/Trackr-A) Other AV vendors detect this malware family with a variety of names, the most common name being *Alina*.

Some of the earliest variants of Trackr had simple functionality that worked like this:

1. Install as a service
2. Use a legitimate-looking name
3. Scan RAM for credit card track one and track two data
4. Dump the results into a text file. This text file was then probably accessed remotely or manually.

Over the years Trackr has become more industrialized, with some cosmetic changes and added bot and network functionality.

Our friends at Trustwave SpiderLabs have written two excellent articles,Alina: Casting a Shadow on PoS and Alina: Following The Shadow, about the inner workings of the Trackr family.

Till now we have observed the following types of Trackr:

- Basic version (not packed, scrapes RAM for credit card information)
- Complex version (added socially-engineered filenames, bot and network functionality)
- Installed DLL version (the DLL is registered as a service and performs the RAM scraping)
- Versions one and two packed with a commercially-available packer
- Versions one and two packed with a custom packer

Most recently, SophosLabs discovered the highly-

prevalent Citadel crimeware targeting PoS systems.

The Citadel malware uses screen captures and keylogging instead of the RAM-scraping technique used by Trackr. Citadel's focus on PoS systems demonstrates that this avenue is fast becoming a point of serious concern.

Who do PoS RAM scrapers target?

One of the earliest serious PoS RAM scraper attacks that we observed was back in November 2011 when we found that a university and several hotels had their PoS systems compromised. Later we saw varied targets including an auto dealership in Australia infected with Trackr.

To better understand the threat we gathered statistics about the various industries targeted by Trackr during the past 6 months (as observed using Sophos Live Protection):

It doesn't come as a surprise that the biggest targeted industries are:

- Retail
- Service
- Healthcare
- Food services
- Education
- Hotel and tourism

In these industries there's a high volume of credit and debit card transactions taking place, meaning they have goldmines of payment data that can be harvested.

Compromising a single PoS system (e.g. in a fast food outlet) may yield thousands of credit cards per week, cheaply – much easier to gather 10,000 credit card details from one PoS system then attempt to infect 10,000 PCs, hoping to grab the data from there.

If not protected properly, PoS systems become easy targets – a single point of failure that can affect thousands of people.

In addition to the breakdown of industries targeted, we also looked at the countries where we saw Trackr infections over the same time period:

Again, no surprises that the developed countries top this chart with the US, where credit cards are abundant, taking the #1 spot.

In fact, the Trackr infection numbers match up closely with the credit card country usage statistics published by Visa.

So how does Trackr get on a PoS system?

We have used the term PoS quite generally throughout this article. PoS is the place where a retail transaction is completed. So a PoS could be some custom hardware/software solution, a regular PC running PoS software, a credit card transaction server, or something similar.

Big box retailers and chain stores have security-hardened PoS systems, and we have not seen any major evidence of these large organizations getting compromised with Trackr.

The victims tend to be mostly small to medium sized organizations who will typically have less investment in defensive counter-measures.

Based on our analysis there were two main methods of infection:

Insider job

Someone with active knowledge of the payment processing setup installs a RAM scraper to gather data. The early Trackr samples dropped their harvested data in a plain text file

which we suspect was manually retrieved or remotely accessed.

The malware had no network functionality and we found no evidence of a top-level dropper/installer.

Phishing/Social Engineering

These are the common infection vectors with the more complex versions of Trackr. The socially engineered filenames we have observed includeTaskmgr.exe, windowsfirewall.exe, sms.exe, java.exe, win-firewall.exe, andadobeflash.exe. This suggests that the files were delivered as part of a phishing campaign, or social engineering tricks were used to infect the system.

Importantly however, Trackr is not seen regularly in the mass-spammed malware campaigns that we observe daily. Rather it is highly targeted towards a group of relevant businesses.

To conclude, it is not always a safe solution to pay for everything with cards.

Everyone should follow computer security best practices and consumers should proactively sign-up for credit monitoring services so they don’t becomes victims of credit or identity theft.

Businesses big and small need to make investments to protect their critical PoS infrastructure. Just like they wouldn’t keep their cash registers unlocked for someone to grab money out of them, PoS systems need proper protection.

Speed Reading Software for GIH Members

Used by the CIA, diplomats, and business professionals to read volumes of info quickly, the Vortex XStream is a simple desktop based application that will flash words on your screen based on a text file, enabling you to read significantly faster and absorb more info than traditional reading.

Think different! How we assimilate information is changing, the computer replaced the book, to a large extent. How we deliver information to our brains is also changing. This method, while developed more than a decade ago, is highly effective, and rarely used.

Download the software here – For GIH Members only – do not share.

Unzip and use – there is no installer. Works in most Windows environments.

From the developer's website:

> *Machine Assisted Reading has come to a computer near you.*
>
> *This software allows humans to read from their computer screens at* ***up to 2000 words per minute.***
>
> *This is accomplished by allowing the separation of the work involved in reading.*
>
> *You set the legibility factors (Font, Size, Color, and Speed of Delivery), sit back, and then the computer does the display, you do the absorption.*
>
> **** Word display at up to 2000 words per minute***
> ** Word display in sizes to the limit of the display*
> ** Word display in any color combination available on your*

display.
** Word display in any typeface font available on your computer.*
** Extract words from all your other software for reading in Vortex xStream with 'soft eyes'.*

Vortex xStream can be used for:

- *Reading text from browsers.*
- *Reading text from email programs.*
- *Reading text from word processing programs.*
- *As a form of tele-prompter.*
- *As a form of text interpreter for the hearing/vision impaired.*
- *As a form of teaching aid for either groups or individually.*
- *As a form of reading enhancement tool for those with *some reading impairments.*

The Vortex xStream software presents one word at a time in the manner best suited to your reading. Your eyes will do less work, and more words will get to the mind.

Vortex xStream is a version of our patented (US Pat. 5,873,109) Machine Assisted Reading Software technology. This version is entirely focused on delivery of speed.

If you need to read vast quantities of text from computers, this software may be for you.

*If you have visual impairments, this software *may be for you. Bear in mind that if you cannot operate software within Windows, you will not be able to operate this software without assistance.*

(This product runs on Microsoft Windows XP, 2000, NT, ME and 98)

Vortex xStream has been used in : Government … Teaching …

> *Spies (CIA) … Business …Schools … Medicine … legal reading … script reading … debugging computer code*

Checkout the developer's blog, Half Past Human.

Hearing: Security Flaws in Obamacare Website Endanger Americans

A panel of IT experts recommended that Americans do not use the healthcare.gov website due to security flaws that could lead to identity theft or worse. The experts said they've 'never seen anything like it' and that it would be easy for a hacker with basic knowledge to break into the site, stealing private data. Their final recommendation as to how to fix it was to scrap the whole project and start from scratch. From freebeacon.com:

> *A panel of IT experts had one answer for Congress when asked if Americans should use the Obamacare exchanges on Healthcare.gov in light of its security concerns: "No."*
>
> *A quartet of experts testifying before the House Committee on Science, Space, and Technology cited numerous security flaws within Healthcare.gov. They attributed the risks to the complexity of its 500 million lines of code and a rushed rollout that failed to properly test the website.*
>
> *David Kennedy, the founder of TrustedSec, an online security firm, said that the risks were easy to ascertain.*

“Just by looking at the website we can see that there is just fundamental security principles not being followed, things that are basic in nature that any security tester, like myself or anyone that we hire to test these sites, would actually test for prior to being released,” Kennedy, formerly of the National Security Agency and a one-time cyber-intelligence analyst for the U.S. Marine Corps, said.

The experts said the personal information of millions of Americans is at risk, including Social Security numbers, birthdays, incomes, home mortgages, and addresses. Rep. Mo Brooks (R., Ala.) called it the “mother lode for identity theft.”

“Americans should be scared to death,” said Rep. Chris Stewart (R., Utah).

Kennedy demonstrated an attack in the hearing room, showing how on Finder.Healthcare.gov a hacker could breach into a computer, monitor its webcam, and steal passwords.

Hackers from Russia or China could “absolutely” breach the online marketplace, he said.

The problems could only get worse since the president’s team is trying to fix the website while it is still up and running.

Morgan Wright, a cyber terrorism expert and CEO of Crowd Sourced Investigations, LLC., said attempting to fix one line of code could open up a “Pandora’s box.”

“You create an unintended series of cascading events you have no control over because you don’t have a grasp of what the code is actually doing,” he said. “You think you’ve changed one thing, by doing that you’ve opened up a Pandora’s box of vulnerabilities on the other side.”

Kennedy said he has never seen anything like it.

“To be honest with you, I have not seen—and I’ve worked for Fortune 10, Fortune 50, Fortune 1,000 companies, as well as on the government side—I have not seen an application that pales in comparison to 500 million lines of code, including some of the largest applications you would ever see in the history of man.”

Because of the sheer amount of code, it is impossible to conduct a complete end-to-end security assessment on the website, the panelists said. Just reviewing it for security risks could take six months.

Fixing the flawed code will also be extremely expensive. The market value of high-end website code is about $50 per line, Kennedy said.

“That’s where I’ve been trying to get my head around, just—half a billion lines of code, particularly when you’re reaching out and pulling it out of other databases and then standardizing,” said Rep. David Schweikert (R., Ariz.). “Does something seem almost absurd?”

“Well, there’s also another paradigm, too, that it costs you $1 to fix it before you launch, it will cost you up to $100 to fix it after you launch,” Wright said.

Another concern is that the website is integrated with other federal agencies, including the Internal Revenue Service (IRS).

“It hooks into the IRS, it hooks into DHS, it hooks into Experian, which is a third party,” Kennedy said. “You have all of these trusted connections, all these things that make up the site itself, but the pieces that actually make up Healthcare.gov are multiple areas.”

“Given Healthcare.gov’s security issues, and assuming for the moment that you would be personally responsible for all damages incurred from your advice, would any of you advise an

American citizen to use this website as the security issues now exist?" asked Rep. Brooks.

Every witness said no.

Kennedy offered three recommendations to Congress. The best option, he said, is to create "Healtcare.gov 2.0," a completely redesigned second website that will work in conjunction with the original. He estimated it would take about six months to complete.

The other options are to take the website offline to fix it, which could take four to six months, or introduce new code while it's still running, which could take years.

"I'm not a political person, I'm not here to talk politics, but if you're asking me from a technology standpoint, it would be easier to start over again, lay the foundation of security, and start from the beginning," Wright said. "The security has to be the foundation of this site. Period."

"Unfortunately the personal information that has already been entered into Healthcare.gov is vulnerable to online criminals and identity thieves," Committee Chairman Lamar Smith (R., Texas) said. "President Obama has a responsibility to ensure that the personal and financial data collected as part of Obamacare is secure. It is clear this is not the case."

"There is only one useable course of action: Mr. President, take down this website."

This debacle needs no comment, healthcare.gov is supposedly the site Americans will be forced to register for, which as it stands now, can expose the private data of every citizen (not only health records but the site is tied to Experian, the IRS, and other databases).

Skype under investigation in Luxembourg over link to NSA

Skype is being investigated by Luxembourg's data protection commissioner over concerns about its secret involvement with the US National Security Agency (NSA) spy programme Prism, the Guardian has learned.

The Microsoft-owned internet chat company could potentially face criminal and administrative sanctions, including a ban on passing users' communications covertly to the US signals intelliigence agency.

Skype itself is headquartered in the European country, and could also be fined if an investigation concludes that the data sharing is found in violation of the country's data-protection laws.

The Guardian understands that Luxembourg's data-protection commissioner initiated a probe into Skype's privacy policies following revelations in June about its ties to the NSA.

The country's data-protection chief, Gerard Lommel, declined to comment for this story, citing an ongoing investigation. Microsoft also declined to comment on the issue.

Luxembourg has attracted several large corporations, including Amazon and Netflix, due to its tax structure.

Its constitution enshrines the right to privacy and states that secrecy of correspondence is inviolable unless the law provides otherwise. Surveillance of communications in Luxembourg can only occur with judicial approval or by authorisation of a tribunal selected by the prime minister.

However, it is unclear whether Skype's transfer of communications to the NSA have been sanctioned by Luxembourg through a secret legal assistance or data transfer agreement that would not be known to the data protection commissioner at the start of their inquiry.

Microsoft's acquisition of Skype tripled some types of data flow to the NSA, according to top-secret documents seen by the Guardian.

Microsoft bought Skype for $8.5bn (£5.6bn) in 2011.

The US software giant was the first technology group to be brought within the NSA initative known as Prism, a scheme involving some of the internet's biggest consumer companies passing data on targeted users to the US under secret court orders.

Having once been considered a secure chat tool beyond the reach of government eavesdropping, Skype is now facing a backlash in the wake of the Prism revelations.

"The only people who lose are users," says Eric King, head of research at human rights group Privacy International. "Skype promoted itself as a fantastic tool for secure communications around the world, but quickly caved to government pressure and can no longer be trusted to protect user privacy."

Skype's legacy of encryption and security

Founded in Scandinavia in 2003, Skype was designed to connect callers through an encrypted peer-to-peer internet connection, meaning audio conversations between Skype users are not routed over a centralised network like conventional phone calls. Video and chat connections are also encrypted.

Attracting millions of users worldwide – 12.9 million people

had registered to use the service by 2004, and by 2011 that figure had reached more than 600 million – Skype's reputation for privacy and security led to it being adopted by journalists and activists as a tool to evade government surveillance. But some criminals, too, turned to the tool to dodge law enforcement agencies – frustrating police, who had previously been able to eavesdrop on suspects' conversations by 'wiretapping' phone lines.

A turning point came in 2005, when US company eBay purchased Skype for $2.6bn (£1.6bn). The same year, Skype formed a joint venture with Hong Kong-based internet company Tom Online to launch a Chinese version of Skype, which was tweaked to be compliant with dragnet surveillance.

Skype China customised for monitoring

A former Skype engineer, who declined to be named because of the sensitive nature of the issue, told the Guardian that the company worked to build in a "listening element" to help Chinese authorities monitor users' communications for keywords, triggering a warning to alert the government when certain phrases get typed into its chat interface.

In response to questions about suspected monitoring of Skype chats in China, Skype has previously stated that its software is made available in the country "through a joint venture with Tom Online. As majority partner in the joint venture, Tom has established procedures to meet its obligations under local laws."

While publicly insisting it was unable to help law enforcement agencies eavesdrop on calls, Skype set up a secretive internal initiative called "Project Chess" to explore how it could make calls available to authorities, according to a New York Times report published in June.

A year later, Skype was purchased from eBay by an investor group including US private equity firms Silver Lake and Andreessen Horowitz. During this period, work began on integrating Skype into the NSA's Prism program, documents leaked by NSA whistleblower Edward Snowden have revealed.

The first 'eavesdropped' Skype call

In February 2011, according to the NSA files, Skype was served with a directive to comply with NSA surveillance signed by the US attorney general. Within days, the spy agency reported that it had successfully eavesdropped on a Skype call. And when Microsoft acquired Skype in May 2011, the relationship with the NSA appears to have intensified.

Caspar Bowden, who served as Microsoft's chief privacy adviser between 2002 and 2011 and left shortly before the completion of its Skype takeover, says he was not surprised to learn the company had complied with the NSA's surveillance of the chat tool.

While working for Microsoft, Bowden says he was not privy to details of secret data-collection programs – but fully briefed the company on the dangers of US spy law the Foreign Intelligence Surveillance Act (FISA) for the privacy of its international cloud customers. He was met with a "wall of silence," he says.

A letter obtained by the Guardian, sent by Skype's corporate vice president Mark Gillett to Privacy International in September 2012, suggested that group video calls and instant messages could be obtained by law enforcement because they are routed through its central servers and "may be temporarily stored."

But Gillett also said in the letter that audio and one-to-one video calls made using Skype's "full client" on computers were encrypted and did not pass through central servers – implying

that the company could not help authorities intercept them.

Separately, in July 2012, Skype contributed to UK parliamentary committee hearings on the government's proposed expansion of surveillance powers under the controversial communications data bill. Skype representative Stephen Collins claimed in testimony to the committee that "there are no keys held by Skype to decrypt communications."

Microsoft calls for more government transparency

Skype told the Guardian that it would not answer technical questions about how it turns over calls to the authorities or comment on the extent of its compliance with US surveillance. The company insisted the information it provided the UK parliament was accurate, though would not explain apparent discrepancies between its public statements and access to Skype calls claimed by the NSA.

In a statement, Skype said it believed that the world needed "a more open and public discussion" about the balance between privacy and security but accused the US government of stifling the conversation.

"Microsoft believes the US constitution guarantees our freedom to share more information with the public, yet the government is stopping us," a spokesperson for Skype said, referring to an ongoing legal case in which Microsoft is seeking permission to disclose more information about the number of surveillance requests it receives.

However, the law that underpins the Prism program – FISA – allows the NSA to target not only suspected terrorists and spies, but also "foreign-based political organisations," which could encompass an array of advocacy groups and potentially news organisations, too.

‘Journalists should avoid Skype’

Grégoire Pouget, an information security expert at Reporters Without Borders, believes that journalists should not underestimate the risks posed by NSA Skype surveillance.

“It is what many of us feared, and now we know for sure,” Pouget says. “If you are a journalist working on issues that could interest the US government or some of their allies, you should not use Skype.”

Although the NSA has access to at least some Skype calls, it remains unclear whether police and security agencies outside the US enjoy a similar level of access.

Hacking Team, an Italian company, sells surveillance software to law enforcement and intelligence agencies in 30 countries that allows authorities to covertly infiltrate computers with spyware that records communications before they are encrypted. The Milan-based firm explicitly markets the Trojan tool as a means to get access to Skype conversations – and says authorities still frequently complain about a lack of ability to eavesdrop on Skype calls.

“When you talk to law enforcement about what their concerns are, they’ll right away mention Skype,” says Eric Rabe, Hacking Team’s spokesman.

Rabe declines to name customers, citing confidentiality agreements, but says Hacking Team’s business has been “growing very nicely” in recent years. The company’s public accounts show that its revenue more than doubled from $5.3m in 2010 to a projected $11.8m in 2012.

The new wave of encrypted services

At the opposite end of the spectrum, new companies are now emerging in response to fears about surveillance of Skype,

promising users access to encrypted chat tools that do not have secret ‘backdoors’ for NSA surveillance.

Washington DC-based Silent Circle is one such company, going to extraordinary lengths to shield customers against spying. With founders including Phil Zimmermann, who devised the Pretty Good Privacy (PGP) email encryption product, and a former Navy Seal, Silent Circle offers a series of encrypted phone apps and a Skype-style internet chat platform.

It is registered as an offshore company and uses computer servers outside the US in a bid to evade government coercion. It recently closed its own encrypted email service because it could not guarantee security, and said it would focus instead on chat and telephony.

The FBI has already held meetings with Silent Circle, according to CEO Mike Janke, accusing it of being a “ghost provider” that could cause harm to the US because it stores virtually no information about its users’ communications.

But Janke, a 45-year-old former Navy Seal sniper, says his company will not cede to government pressure to secretly comply with surveillance. “I feel that we can use Skype as a template,” Janke says, “for what we don’t want to do.”

http://www.theguardian.com/technology/2013/oct/11/skype-ten-microsoft-nsa

---

Synchronize your Meta Trader folders

Elite Meta Sync synchronizes your files between MT4

installations as well as creating a backup in your My Documents folder.

Elite Meta Sync will sync your experts, indicators, dlls, libraries, and other files between all MT4 terminal installations.

This tool is offered free for Global Intel Hub members only. Do not share this tool or resell it. You may use it on as many computers as you wish.

EES_MetaSync download

Unzip, and install – it's fairly self explanatory, but a help file is included which can be accessed once the application is launched.