Computer Security

19. After the attack

Paul Krzyzanowski

Rutgers University

Spring 2018

Sometimes attackers win

Systems get compromised

- Why?
  - 0-day attacks
  - Social engineering attacks
  - Carelessness in configuration
  - Poor defenses
  - Lack of patches
  - Malicious insiders
  - …
- How do you recover

Be paranoid

- Paranoia
  - It can be extremely difficult to clean an infected system
  - Well-analyzed malware may be undone
  - But it is easy to install back doors
  - General advice: reformat & reinstall
- Extra paranoia
  - Malicious firmware in peripheral devices, EFI/BIOS
  - Maybe throw away the hardware?

If you throw away the computer

- If the file system is not encrypted, an attacker can
  - Retrieve files
    - Email, messages
    - Network configuration
    - User names & hashed passwords
    - Browsing history
  - Reconstruct deleted files

Hidden back doors sitting in various places

- cron jobs
- Modified standard system services … or new ones
  - There are at least 6 different ways to start programs at boot time on Windows!
  - *launchd* on macOS; *systemd* on Linux
- Many others…
- Self-repairing malware
  - Two or more programs with back doors
  - Each checks the other
  - If one is deleted, the other adds it back

Bots

- Some infections turn machines into bots
- Bot software can upgrade itself
  - Download different payloads
    - spam engines, DDoS attackers, keystroke loggers
- Often install rootkits to prevent detection
  - Try to prevent anti-virus software from detecting them

Backups

- Frequent backups are a must
- Recover data but not programs from backups
  - Still a danger of infected data, such as MS-Word documents
- Backups must be tested
  - Make sure recovery process works!
  - Keep offsite backups too

Tripwire

- Create checksums (hashes) of each file
  - Recalculate checksums and compare stored files
  - Detect unexpected changes to files
  - Not always easy since some files change frequently
    - And what if malware modifies the tripwire database?
- Safer but more complex
  - Store the checksum file on different media
  - Use another system to read the disk that you're checking
  - Do not trust any software on the possibly-compromised machine

Analyzing a hacked computer

- Work with a copy – preferably an image of the disk
  - Don't destroy the metadata – e.g., file access times
- Mount the image with *noexec* and *nodev* options
- Search for files that were changed recently
  - Look at *ctime* (change time) in addition to *mtime* (modification time)
    - *ctime* = updated when metadata changes even if file contents don't change
  - Compare with tripwire checksums

Log files

- Log to external systems – preferably protected by a firewall
  - Attackers can wipe logs
- Check logs for suspicious entries
- Outbound connections from infected machines can indicate attempts to spread malware
- Earlier inbound connections to the machine can show where and how the problem started

Suspicious new files

- File names that resemble legitimate files
  - C:\Windows\Windows Explorer.exe
- Strange names
  - … (3 dots)
  - "bin " (space after the name)
  - " .exe"

Deleted files

- Deleting a file does not delete its data
- i-node and data blocks are just marked as free
- Tools can recover deleted files
- "secure delete" operations will wipe the data blocks
  - Apple removed Secure Empty Trash in OS X El Capitan
    - There was a bug where it might not securely delete the file data

Deleted blocks

- Solid-state drives will try to do wear-leveling and not reuse the same blocks for a while
  - "Overwriting" a block in a file may result in the allocation of a new block
- Magnetic disks leave a trace
  - Magnetic disks are an analog system
    - If a "1" is written over a "0", it's sort of like 0.95
    - If a "1" is written over a "1", it's sort of like 1.05
  - It has been claimed that Magnetif Force Scanning Tunneling Microscopy can retrieve this data
  - No definitive proof it works
    - We think intelligence agencies can do this (but it's tedious!)

Memory dumps

- If the system is up, dump the memory (/dev/kmem)
- Malware can often be found in plaintext in memory
  - Decryption keys for encrypted file systems can often be found there

Are we safe?

All we need are:

- Educated users – don't be a phishing victim
- Permissions, containers, ASLR, stack canaries, no-execute stack
- Good programming: bounds checking, input sanitization
- Encrypted storage
- Host-based firewalls
- Network firewalls and intrusion detection systems
- Cryptographic authentication & communication

Are we safe?

What happened over the past 1+ months?

March 6-8: Cryptomining

- "Several sophisticated trojans" spreading rapidly across Russia, Turkey and Ukraine
- Malware carries "coin miner payload"
- Upon infection:
  - Connects to a hacker's command and control server
  - Listens for commands, including installation of additional malware
  - Replaces legitimate Microsoft IE with covert malware
- Malware around since 2011

March 6: Cortana bypasses passwords

Researchers Bypassed Windows Password Locks With Cortana Voice Commands

Two independent Israeli researchers found a way for an attacker to bypass the lock protection on Windows machines and install malware by using voice commands directed at Cortana.

March 6: Exim bug

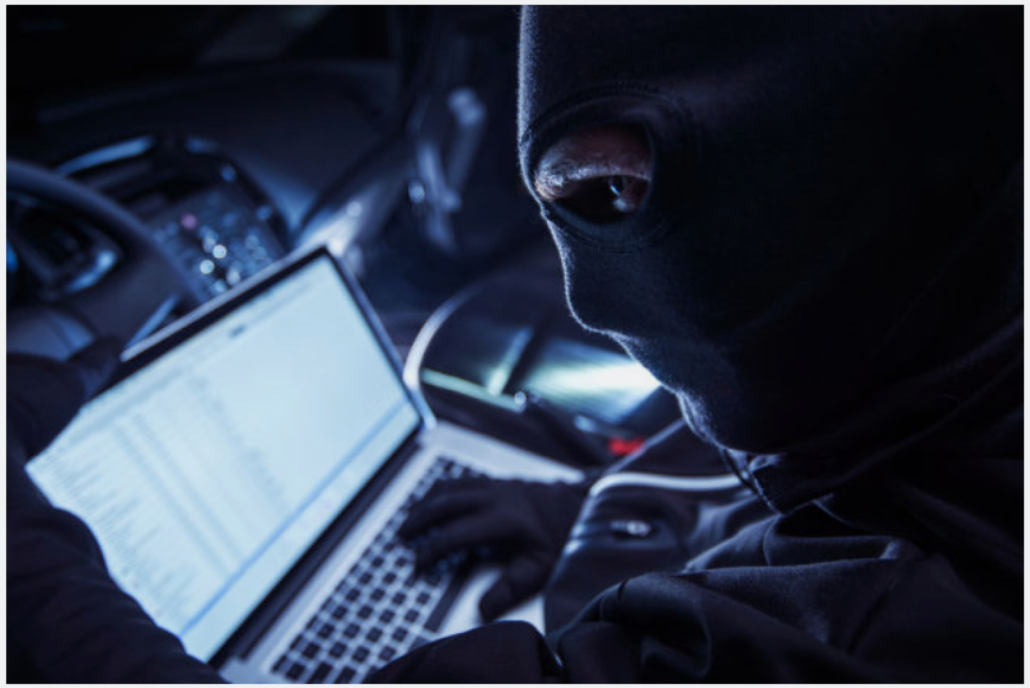
- Exim message transfer agent
- Opens servers to attacks that can execute malicious code
- Buffer overflow vulnerability

TAKE COVER —

400k servers may be at risk of serious code-execution attacks. Patch now

Widely used message transfer agent patched buffer overflow last month.

DAN GOODIN - 3/6/2018, 7:45 PM

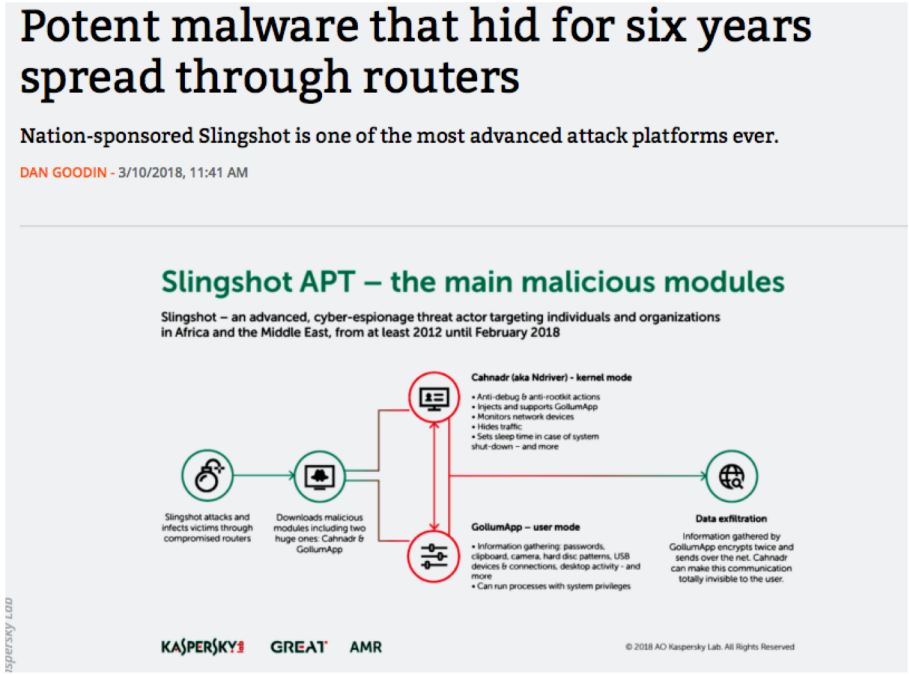


Thinkstock Photos

Hacker stock photos FTW.

March 10: Slingshot APT

- Infected at least 100 computers
  – hidden for 6 years
- Highly advanced
  – Loads signed vulnerable drivers
  – Runs its code through their vulnerabilities
  – Then loads kernel and user modules
  – Sets up an encrypted file system an unused part of the disk
- Designed for espionage
  – Collects screenshots, keyboard/network/USB data, passwords



Potent malware that hid for six years spread through routers

Nation-sponsored Slingshot is one of the most advanced attack platforms ever.

DAN GOODIN - 3/10/2018, 11:41 AM

Slingshot APT – the main malicious modules

Slingshot – an advanced, cyber-espionage threat actor targeting individuals and organizations in Africa and the Middle East, from at least 2012 until February 2018

KASPERSKY GREAT AMR

March 14: IoT

You Can Hack Almost Any Smart Device With A Google Search

The internet of things is so poorly designed that you can gain control of devices just Googling for passwords.

- Hacking IoT can be easy – just do a Google search
- "within a few minutes, you will find a site or a forum post somewhere describing how to enter into that device using the manufacturer's default administration user name and password. "

March 13: Power utilities

"An American power company has reached a settlement to pay an unprecedented $2.7 million penalty over significant security oversights that could have allowed hackers to gain remote access to the power provider's systems."

"A security researcher discovered more than 30,000 company records online unprotected by even a password."

US Power Company Fined $2.7 Million Over Security Flaws Impacting 'Critical Assets'

Dell Cameron
3/13/18 6:25pm • Filed to: SECURITY

10.6K 13 3

Photo: AP

March 15: Trojan: BitTorrent backdoor

- Malware tried to install a cryptocurrency miner
- Sneaked malware into a BitTorrent application called Mediaget
- Windows Defender blocked >400K instances

March 23: Atlanta ransomware

Atlanta government computers hit by ransomware

The attackers are reportedly demanding $50k in bitcoin.

- SamSam malware disrupted 13 local government departments
  - Crippled court system
  - Disallowed water bill payment
  - Hurt sewer infrastructure requests & police reports
- Scan-and-exploit propagation techniques
  - Targets passwords, JBoss, RDP (remote desktop protocol), others
- First identified in 2015

March 29: Drupal bug

Drupal CMS vulnerability allows hackers to gain complete control of your website

The input sanitation vulnerability, an oversight that allows for arbitrary code execution, was patched on Wednesday by Drupal developers.

By James Sanders | March 29, 2018, 5:36 AM PST

An oversight that led to inputs not being sanitized was patched on Wednesday by Drupal.

*The vulnerability is extremely trivial to exploit, making patching active installations critical.

A failure to sanitize inputs prompted a round of emergency patching for Drupal on Wednesday. The patch was announced a week in advance to give administrators time to prepare due to concerns that exploits "might be developed within hours or days" of the release of the patch.

April 1: Yet another credit card heist

Card Data Stolen From 5 Million Saks and Lord & Taylor Customers

By Vindu Goel and Rachel Abrams
April 1, 2018

Saks has been hacked — adding to the already formidable challenges faced by the luxury retailer.

A well-known ring of cybercriminals has obtained more than five million credit and debit card numbers from customers of Saks Fifth Avenue and Lord & Taylor, according to a cybersecurity research firm that specializes in tracking stolen financial data. The data, the firm said, appears to have been stolen using software that was implanted into the cash register systems at the stores and that siphoned card numbers until last month.

The Hudson's Bay Company, the Canadian corporation that owns both retail chains, confirmed on Sunday that a breach had occurred.

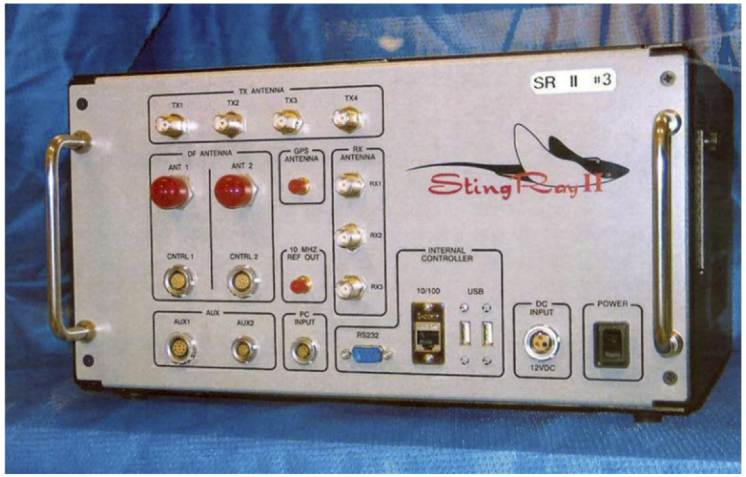
April 4: Surveillance devices

- The Department of Homeland Security says it has seen activity in Washington, D.C., of what appear to be rogue surveillance devices that could be used to hijack cellphones, listen to calls and read texts.
- But it says it's not able to actually track down where they are, because that would require more funding.
- It's not clear who is deploying the unauthorized devices, which are known as IMSI catchers or Stingrays and may legally be sold only to public safety and law enforcement officials.

Feds Say They've Detected Apparent Rogue Spy Devices In D.C.

April 4, 2018 · 4:57 PM ET

MERRIT KENNEDY



The Department of Homeland Security detected "anomalous activity" consistent with cellular site simulators such as the StingRay II.

U.S. Patent and Trademark Office via AP

April 5: Network hardware bugs

MY USERNAME IS "RM -RF *.*" —

"Open sesame": Industrial network gear hackable with the right username

Vulnerabilities in two devices from Moxa show security to be an afterthought.

SEAN GALLAGHER - 4/5/2018, 5:49 PM

This week, two separate security alerts have revealed major holes in devices from Moxa, an industrial automation networking company.

In one case, attackers could potentially send commands to a device's operating system by using them as a username in a login attempt.

In another, the private key for a Web server used to manage network devices could be retrieved through an HTTP GET request.

April 11: Hacked websites

UNWITTING PARTICIPANTS —

Thousands of hacked websites are infecting visitors with malware

Unusually advanced campaign infects people visiting a variety of poorly secured sites.

DAN GOODIN - 4/11/2018, 7:15 AM

Thousands of hacked websites have become unwitting participants in an advanced scheme that uses fake update notifications to install banking malware and remote access trojans on visitors' computers, a computer researcher said Tuesday.

The campaign, which has been running for at least four months, is able to compromise websites running a variety of content management systems, including WordPress, Joomla, and SquareSpace.

April 15: Smart thermostat

Hackers exploit casino's smart thermometer to steal database info

Share on Facebook | Share on Twitter | +

A casino in Las Vegas.

IMAGE: MICHEL RATHWELL/FLICKR

April 16: IoT … again

LILY HAY NEWMAN SECURITY 04.16.18 01:00 PM

AN ELABORATE HACK SHOWS HOW MUCH DAMAGE IOT BUGS CAN DO

Attackers can jump from one vulnerable IoT device to the next, totally bypassing mainstream devices like PCs and servers, and charting a course that's much harder to detect.

Demos used publicly-known exploits

- Compromise a camera
- Use that to discover the router's IP address & type
- Crack router's hashed password to access router
- Router can then "phone home" to get more commands
- Change network rules at will

April 19: DoS

Answer Sheet

Computer glitches interrupt standardized testing in states across the country

By Valerie Strauss April 19 Email the author

In Tennessee, an attack on a software vendor interrupted standardized testing this week and may have also caused delays in Mississippi. In Ohio, computers crashed statewide as students were getting ready to take that state's tests. In New York, computers went down, too, affecting students in several ways, and in one New York school district, a superintendent slammed some of the questions.

April 21: iPhone cracking

Stop Using 6-Digit iPhone Passcodes

Now that police agents can allegedly crack iPhones protected with passcodes made of six numbers, it's time to use longer, harder to guess and crack alphanumeric passphrases.

April 26: World's largest DDoS-for-hire service

engadget

Police take down the world's largest DDoS-for-hire service

WebStresser launched denial of service attacks for as little as $15.

Jon Fingas, @jonfingas • April 26, 2018

The internet might be slightly safer against distributed denial of service attacks in the near future... slightly. Police in twelve countries have taken down WebStresser, believed to be the world's largest service for paid DDoS attacks. The joint campaign (Operation Power Off) seized WebStresser's infrastructure in the US, UK and the Netherlands, and busted site administrators ranging as far as Australia and Hong Kong.

April 21: Alexa

Security Researchers Created a 'Skill' that Allows Alexa to Spy on You

AJ Dellinger
Wednesday 7:37pm • Filed to: AMAZON

34.8K 15 1

Photo: Getty

April 24, 2018: Hackers emptied Ethereum wallets

- Users connecting to MyEtherWallet were presented with an unsigned SSL certificate
  - Many users just clicked through
- Those who clicked through the warning were directed to a server in Russia, who obtained the users' credentials (via login) and emptied their wallets
  - About $150,000 in digital coins was stolen
- **MyEtherWallet was not compromised. What happened?**

1. The attackers compromised the eNet ISP (based in Columbus, OH, AS10297)

2. To capture traffic destined for AWS's Route 53 DNS service, they configured eNet to send more specific (/24 instead of /23) BGP route announcements to its peers (Level 3, Hurricane Electric, Cogent, NTT, …)

3. Attackers then either:
   - Set up a VPN or tunnel between eNet & the target DNS system
   - Set up routing tables at the data center

4. The attackers either ran or compromised a server hosted at an Equinix data center in Chicago that ran a DNS service returning malicious addresses for MyEtherWallet.com.

5. Users accessing MyEtherWallet.com were presented with an IP address to a server in Russia that had a self-signed certificate but some ignored the warnings.

The end