RSACONFERENCE2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Hacking Exposed: Day of Destruction

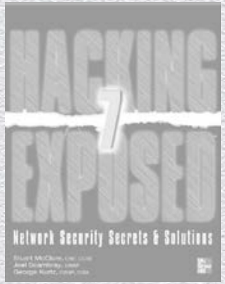
SESSION ID: EXP-W01

George Kurtz
CrowdStrike, President & CEO

Dmitri Alperovitch
CrowdStrike, Co-Founder & CTO

A LITTLE ABOUT US

- George Kurtz, President/CEO & Co-founder
  - In security for 20 +years
  - President & CEO, CrowdStrike
  - Former CTO, McAfee
  - Former CEO, Foundstone
  - Author, *Hacking Exposed*
  - ***@George_Kurtz***



A LITTLE ABOUT US

- Dmitri Alperovitch
  - Co-Founder & CTO, CrowdStrike
  - Former VP Threat Research, McAfee
  - Author of Operation Aurora, Night Dragon, Shady RAT
  - MIT Tech Review's Top 35 Innovator Under 35 for 2013
  - Foreign Policy's Top 100 Leading Global Thinkers for 2013
  - **@DmitriCyber**

A LITTLE ABOUT US

- Alex Ionescu
  - Hardware Hacking Ninja
  - Chief Architect, CrowdStrike
  - Co-author of Windows Internals
  - ReactOS architect
  - **@aionescu**

Agenda

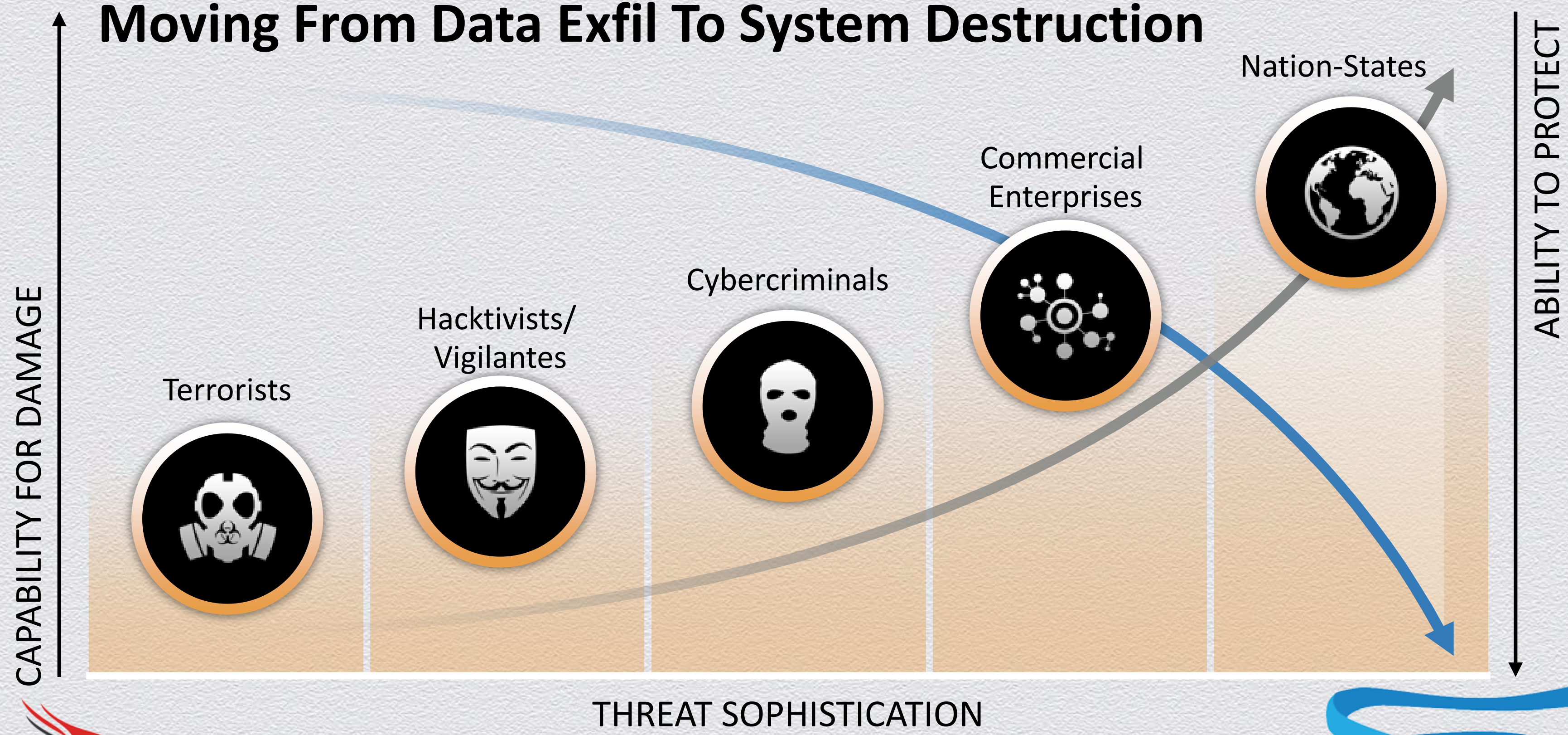
- A Walk Down Memory Lane: Destructive Attacks Throughout History
- Next Generation: Targeted Destructive Attacks
- The Setup
- Demo
- Countermeasures

This presentation contains strong scenes of computer violence, and several systems **were harmed** in the making of this presentation.

Walk Down Memory Lane: Destructive Attacks Throughout History

Adversary is Evolving…

Moving From Data Exfil To System Destruction



Before Photo Bombs – Fork Bombs

- While (1) { fork ();} - Old School

- :(){ :|:& };: - 13 characters of pain - Gangsta Circa 2002

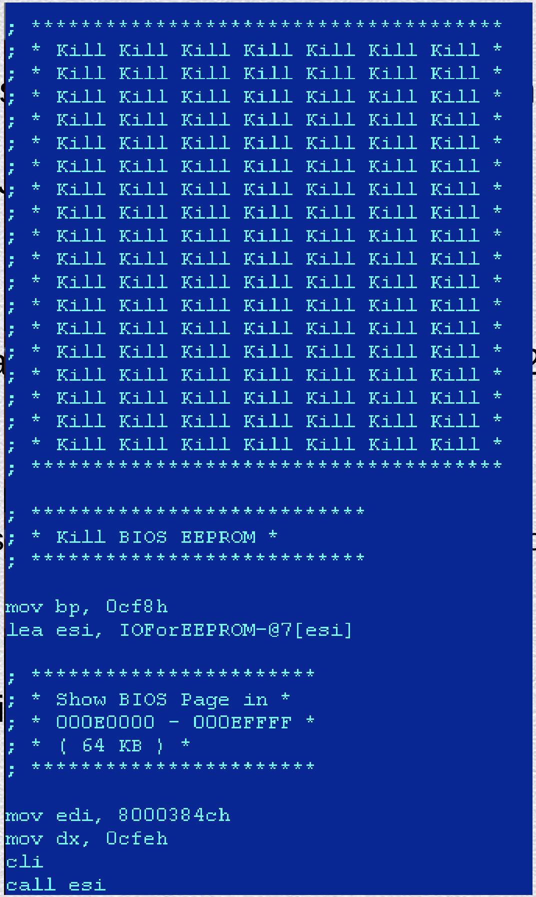
CIH Virus (aka Chernobyl, aka Spacefiller)

- Written in Ass
- Released in J
- Works on Wi
- Infects files a
- Destruction:
  - Overwrites
  - Attempt to
- High sophisti

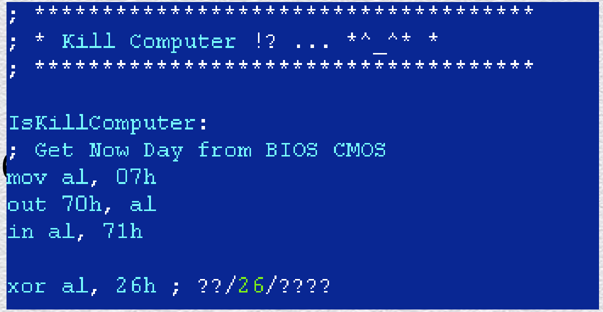
t at Tatung University in Taiwan

2(Chen's birthday)

pes, deletes partition table (recoverable)

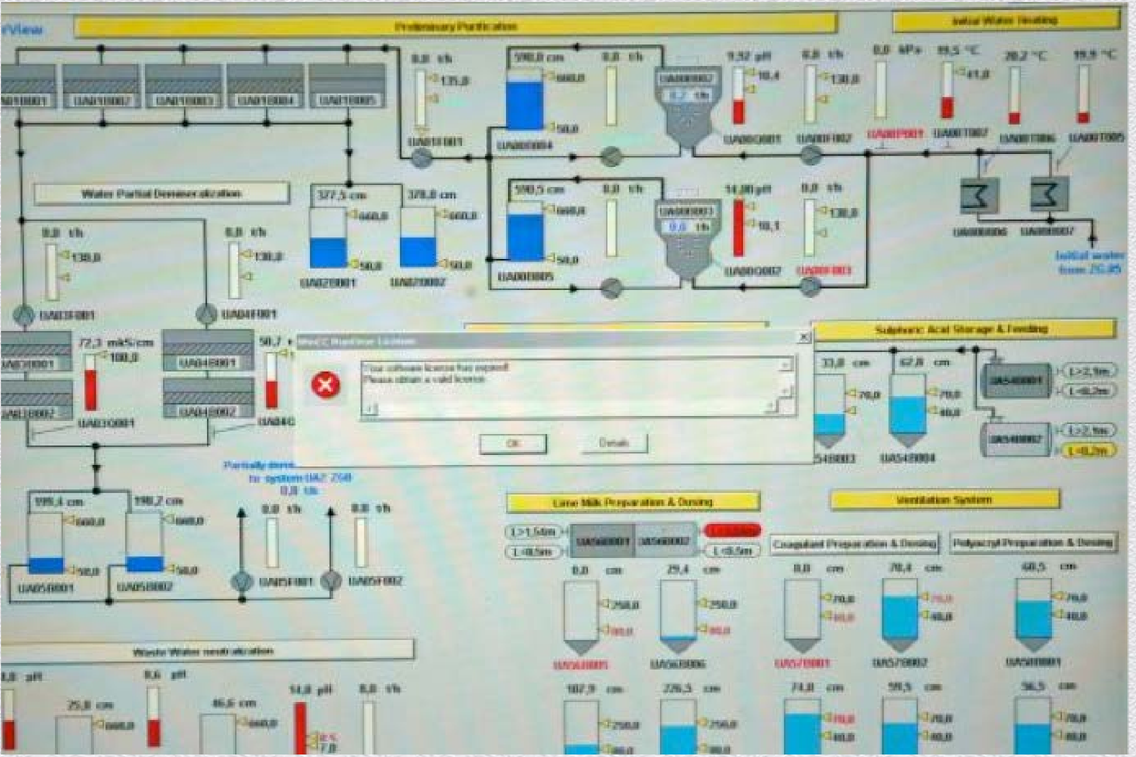


```
; ************************************
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; * Kill Kill Kill Kill Kill Kill Kill *
; ************************************

; **************************
; * Kill BIOS EEPROM *
; **************************

mov bp, 0cf8h
lea esi, IOForEEPROM-@7[esi]

; ***********************
; * Show BIOS Page in *
; * 000E0000 - 000EFFFF *
; * ( 64 KB ) *
; ***********************

mov edi, 8000384ch
mov dx, 0cfeh
cli
call esi
```



```
; ************************************
; * Kill Computer !? ... *^_^* *
; ************************************

IsKillComputer:
; Get Now Day from BIOS CMOS
mov al, 07h
out 70h, al
in al, 71h

xor al, 26h ; ??/26/????
```

Stuxnet

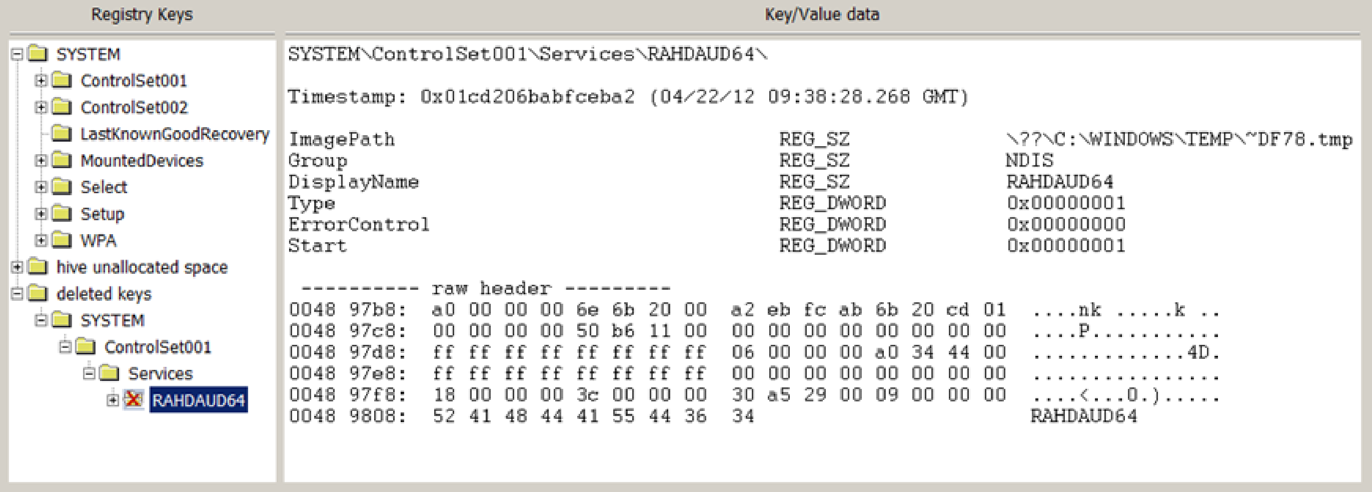


Preliminary Purification
Initial Water Heating
Water Partial Demineralization
Sulphuric Acid Storage & Feeding
Lime Milk Preparation & Dosing
Ventilation System
Coagulant Preparation & Dosing
Polyacryl Preparation & Dosing
Waste Water neutralization
Initial water from 2G.05
OK
Details

Your software license has expired!
Please obtain a valid license.

Wiper

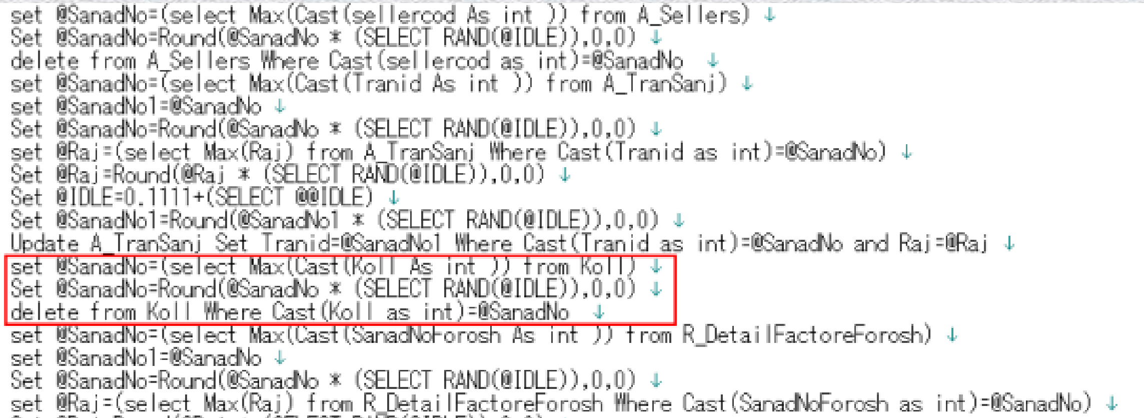
- Indicators discovered by Kaspersky in Iran in April 2012
- Active December 2011-April 2012
- Malware never identified but believed to be high sophistication



```
SYSTEM\ControlSet001\Services\RAHDAUD64\

Timestamp: 0x01cd206babfceba2 (04/22/12 09:38:28.268 GMT)

ImagePath                                 REG_SZ                  \??\C:\WINDOWS\TEMP\~DF78.tmp
Group                                     REG_SZ                  NDIS
DisplayName                               REG_SZ                  RAHDAUD64
Type                                      REG_DWORD               0x00000001
ErrorControl                              REG_DWORD               0x00000000
Start                                     REG_DWORD               0x00000001

 ---------- raw header ---------
0048 97b8:  a0 00 00 00 6e 6b 20 00  a2 eb fc ab 6b 20 cd 01  ....nk .....k ..
0048 97c8:  00 00 00 00 50 b6 11 00  00 00 00 00 00 00 00 00  ....P...........
0048 97d8:  ff ff ff ff ff ff ff ff  06 00 00 00 a0 34 44 00  .............4D.
0048 97e8:  ff ff ff ff ff ff ff ff  00 00 00 00 00 00 00 00  ................
0048 97f8:  18 00 00 00 3c 00 00 00  30 a5 29 00 09 00 00 00  ....<...0.).....
0048 9808:  52 41 48 44 41 55 44 36  34                       RAHDAUD64
```

Narilam

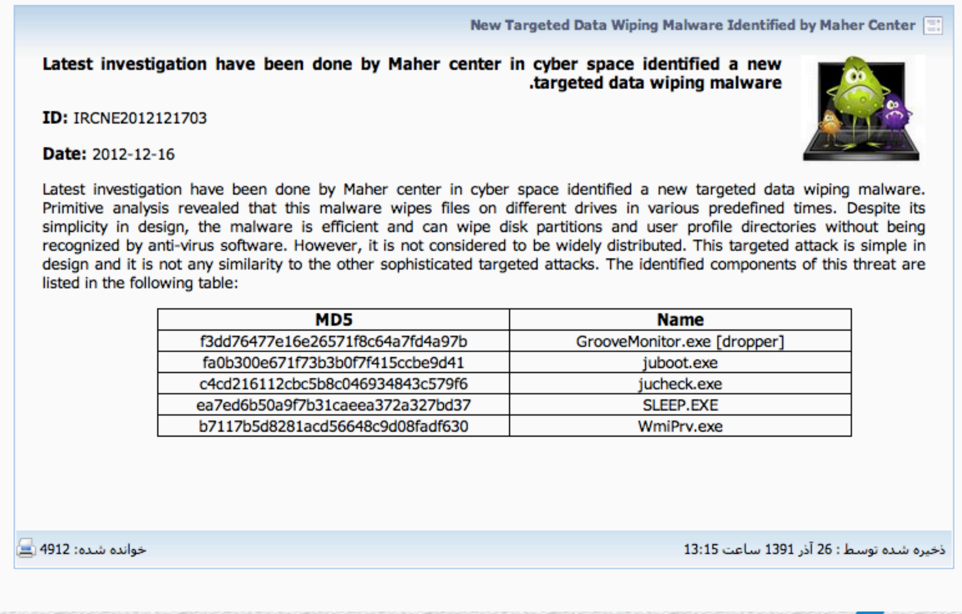
- Discovered by Symantec in November 2012
- Written in Delphi with infections observed almost exclusively in Iran
- Replaced financial data with random values in MS SQL Databases, drops certain tables
- Very low sophistication



```
set @SanadNo=(select Max(Cast(sellercod As int )) from A_Sellers) ↓
Set @SanadNo=Round(@SanadNo * (SELECT RAND(@IDLE)),0,0) ↓
delete from A_Sellers Where Cast(sellercod as int)=@SanadNo  ↓
set @SanadNo=(select Max(Cast(Tranid As int )) from A_TranSanj) ↓
set @SanadNo1=@SanadNo ↓
Set @SanadNo=Round(@SanadNo * (SELECT RAND(@IDLE)),0,0) ↓
set @Raj=(select Max(Raj) from A_TranSanj Where Cast(Tranid as int)=@SanadNo) ↓
Set @Raj=Round(@Raj * (SELECT RAND(@IDLE)),0,0) ↓
Set @IDLE=0.1111+(SELECT @@IDLE) ↓
Set @SanadNo1=Round(@SanadNo1 * (SELECT RAND(@IDLE)),0,0) ↓
Update A_TranSanj Set Tranid=@SanadNo1 Where Cast(Tranid as int)=@SanadNo and Raj=@Raj ↓
set @SanadNo=(select Max(Cast(Koll As int )) from Koll) ↓
Set @SanadNo=Round(@SanadNo * (SELECT RAND(@IDLE)),0,0) ↓
delete from Koll Where Cast(Koll as int)=@SanadNo  ↓
set @SanadNo=(select Max(Cast(SanadNoForosh As int )) from R_DetailFactoreForosh) ↓
set @SanadNo1=@SanadNo ↓
Set @SanadNo=Round(@SanadNo * (SELECT RAND(@IDLE)),0,0) ↓
set @Raj=(select Max(Raj) from R_DetailFactoreForosh Where Cast(SanadNoForosh as int)=@SanadNo) ↓
```

Maya

- Discovered in Iran in December 2012
- Attempts to delete all files on disks D: through I: on certain dates using a BAT file converted to an EXE
- Very simplistic



New Targeted Data Wiping Malware Identified by Maher Center

Latest investigation have been done by Maher center in cyber space identified a new .targeted data wiping malware

ID: IRCNE2012121703

Date: 2012-12-16

Latest investigation have been done by Maher center in cyber space identified a new targeted data wiping malware. Primitive analysis revealed that this malware wipes files on different drives in various predefined times. Despite its simplicity in design, the malware is efficient and can wipe disk partitions and user profile directories without being recognized by anti-virus software. However, it is not considered to be widely distributed. This targeted attack is simple in design and it is not any similarity to the other sophisticated targeted attacks. The identified components of this threat are listed in the following table:

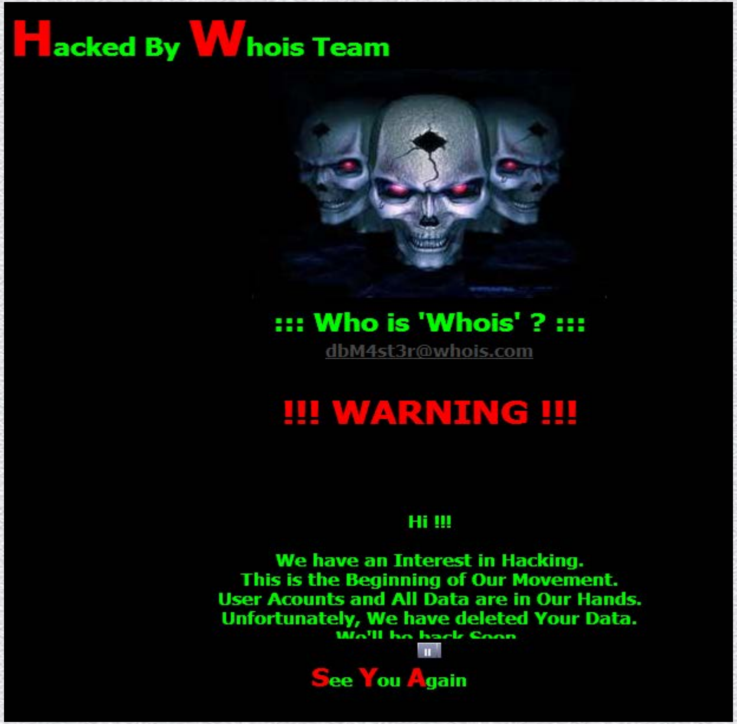
MD5	Name
f3dd76477e16e26571f8c64a7fd4a97b	GrooveMonitor.exe [dropper]
fa0b300e671f73b3b0f7f415ccbe9d41	juboot.exe
c4cd216112cbc5b8c046934843c579f6	jucheck.exe
ea7ed6b50a9f7b31caeea372a327bd37	SLEEP.EXE
b7117b5d8281acd56648c9d08fadf630	WmiPrv.exe

خوانده شده: 4912

ذخیره شده توسط : 26 آذر 1391 ساعت 13:15

Korean / DarkSeoul attacks

- Disk wipers
  - “HASTITI” Wipers
  - “Whois Team” Wipers?
- Simple Backdoor Shells
- Downloaders
- Variety of full featured RATs
- Linked by various TTPs, including:
  - Encryption (methods / keys)
  - Keyword lists
  - File mapping naming conventions



Hacked By Whois Team

::: Who is 'Whois' ? :::

dbM4st3r@whois.com

!!! WARNING !!!

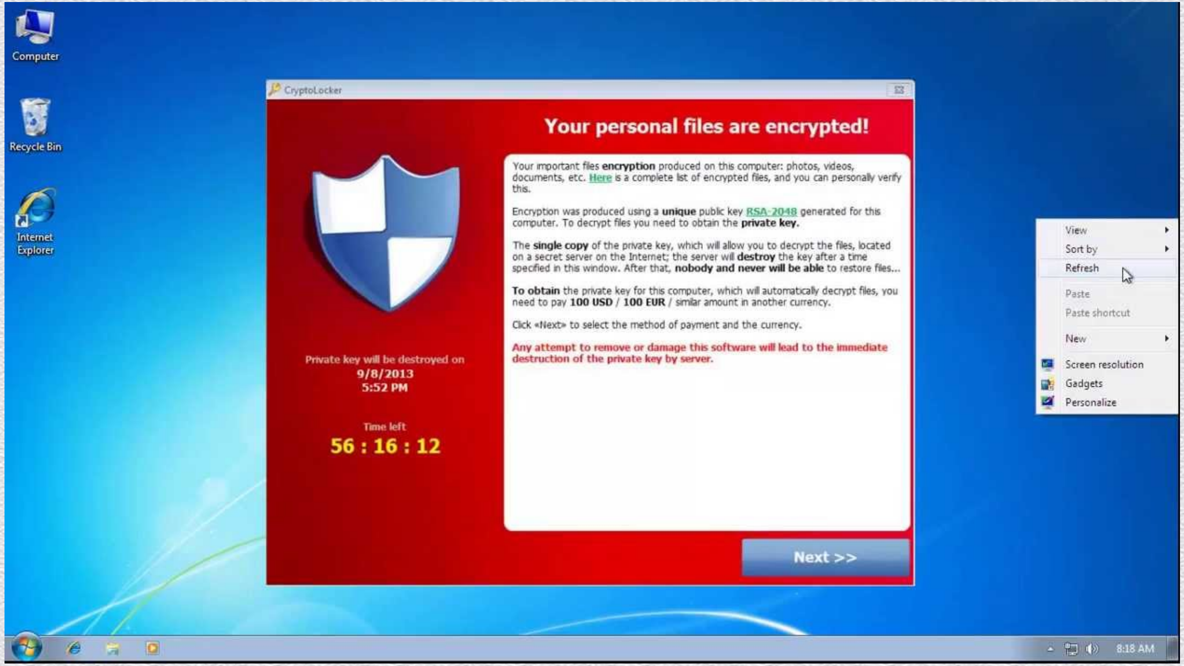
Hi !!!

We have an Interest in Hacking.
This is the Beginning of Our Movement.
User Acounts and All Data are in Our Hands.
Unfortunately, We have deleted Your Data.
We'll be back Soon

See You Again

Ransomware

- AIDS / PC Cyborg Trojan – 1989
- GPCode - 2005
- Cryptolocker - 2013



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD** / **100 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/8/2013
5:52 PM

Time left
56 : 16 : 12

Shamoon

- Responsible for reported 30,000 machines destroyed at Middle East energy companies in August 2012
- Used commercial ElDoS raw disk access kernel driver to overwrite the disk
- Low sophistication

Demo #1

Historic Destructive Attacks Scenarios

Attack Type	Recovery
Data Destruction	Data Backups
Data Encryption	Data Backups
Boot Impact	
• Overwrite HD MBR & Partition Table	HD Backups, partition table restoration programs
• Reflash BIOS	BIOS signing, reflash back

NEXT-GENERATION:
PERMANENT DESTRUCTION

ATTACKING
THE HARDWARE

Devastation Impact: Imagine if…

- You walk in the building and your badge doesn't work
- The HVAC is off
- The security cameras are shutdown
- 50,000 monitor screens are blinking 'System disk error'
- Phone systems & video conferencing are down
- Mail servers are down
- VPN is down
- And you can't get your coffee because the CC reader is down

The Setup

Permanent Destruction Scenarios

Fry Battery: very hard to do now

Keyboard Firmware: recoverable

Camera Firmware: recoverable

Touchpad firmware: recoverable

LCD Screen firmware: recoverable

SSD Controller: have to reflash without relying on data

Video Card: have to reflash without relying on graphics

Thunderbolt Controller: have to reflash -- can prevent external disk/video card/monitor from working in recovery scenarios above

EFI/BIOS: hard to recover

ACPI EC (Embedded Controller): hard to recover

Intel ME: hard to recover

Setup

- Went after the most realistic (time/effort) target with the biggest impact and recovery difficulty:
  - ACPI Embedded Controller (ACPI EC)
- ACPI EC sits on the LPC Bus (replacement for legacy ISA Bus)
  - Has its own flash and processor (usually an MCU like STM-32, ARM Cortex, Hitachi SH3/H8300)
- Controls LCD/keyboard backlight, power button, I2C battery bus, charging circuit, LEDs, fans, thermal monitoring and power throttling
  - Corrupted/dead ACPI EC would result in up to the inability to power on and/or charge the machine and/or use its battery

Setup

- Most ACPI chips are not frequently updated by their manufacturers
- Some laptops have open-source chip firmware and updater
- Apple computers have closed-source chip firmware
- We modified an existing Apple firmware update for their chip and corrupted it

Frying the Machine

- Turn off the fans
- Spike the CPU to 100%
- Watch the temperature rise to boiling water level

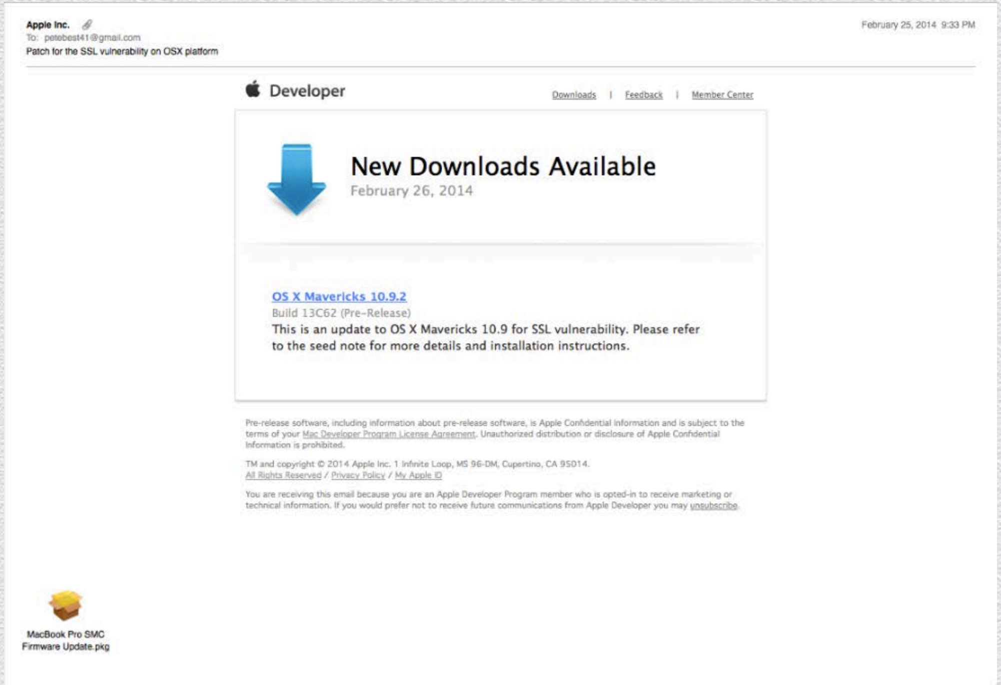
- Impact
  - Burn the laptop owner
  - Permanently damage internal electronics
  - …Or start a fire if the electronics are shoddy

Demo #2

Main Attack Scenario

Day of Destruction

- **Background**: Apple SSL vulnerability in the news
- Last week of the quarter – CEO pushing for the last deals
- Social Engineer a victim to apply an Apple OSX patch
- Update the ACPI firmware and reboot the machine
- Watch the machine lockup during the update
- Reboot renders the machine unbootable



Apple Inc.
To: petebest41@gmail.com
Patch for the SSL vulnerability on OSX platform

February 25, 2014 9:33 PM

Developer

Downloads | Feedback | Member Center

New Downloads Available
February 26, 2014

OS X Mavericks 10.9.2
Build 13C62 (Pre-Release)
This is an update to OS X Mavericks 10.9 for SSL vulnerability. Please refer to the seed note for more details and installation instructions.

Pre-release software, including information about pre-release software, is Apple Confidential information and is subject to the terms of your Mac Developer Program License Agreement. Unauthorized distribution or disclosure of Apple Confidential information is prohibited.

TM and copyright © 2014 Apple Inc. 1 Infinite Loop, MS 96-DM, Cupertino, CA 95014.
All Rights Reserved / Privacy Policy / My Apple ID

You are receiving this email because you are an Apple Developer Program member who is opted-in to receive marketing or technical information. If you would prefer not to receive future communications from Apple Developer you may unsubscribe.

MacBook Pro SMC Firmware Update.pkg

Result: You have thousands of expensive doorstops in your enterprise and not a single working machine

WARNING!

- DO NOT TRY THIS AT HOME!

- MULTIPLE MACHINES WERE DESTROYED IN THE MAKING OF THIS DEMO

Demo #3

Countermeasures

- Firmware signing
- Windows 8 includes EFI signing (NIST BIOS Protection Guidelines)
- Vendors need to sign all firmware

- Free tool release: CrowdResponse

Introducing CrowdResponse

- Free incident response collection and detection tool from CrowdStrike
- Announced today and will be released next week
- Scans **per-process memory** and disk images with Yara rules
- Supports all modern Windows platforms – WinXP → Server 2012
- Configuration file currently manages over 40 different output options resulting in nearly 100 possible data points
- Command-line based and easy to deploy at scale
- XML output – CRconvert tool provides CSV and HTML reports

First 3 CrowdResponse Modules

@pslist

- List all processes
- Collect PE header
- Verify digital signatures
- Hash image binary
- Process command line
- Loaded DLLs
- Imports/exports
- Identify code injection

@dirlist

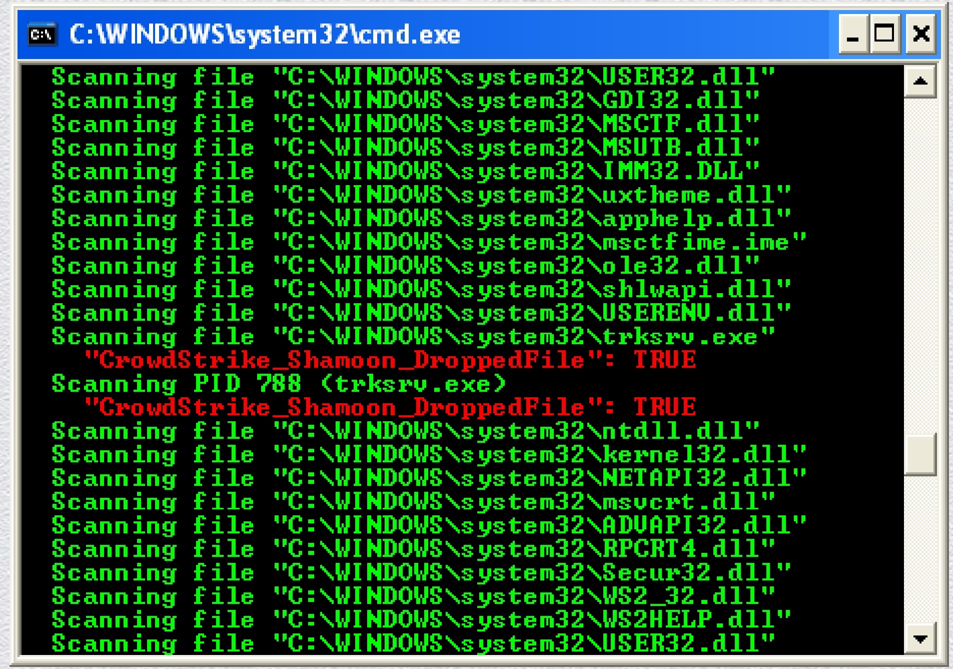
- Recursive file listing
  - Regex masks
  - Recursion limits
- Verify digital signatures
- MD5/SHA256 hashes
  - Quick hash capable
- Collect resource info
- Timestamp collection

@yara

- Scan memory
  - All running processes
  - On-disk image binaries
  - DLLs
- Yara rule management
  - Download rules from URL
  - Rule masks
- Limit scanning by regex

Detecting the Shamoon Dropper with @yara

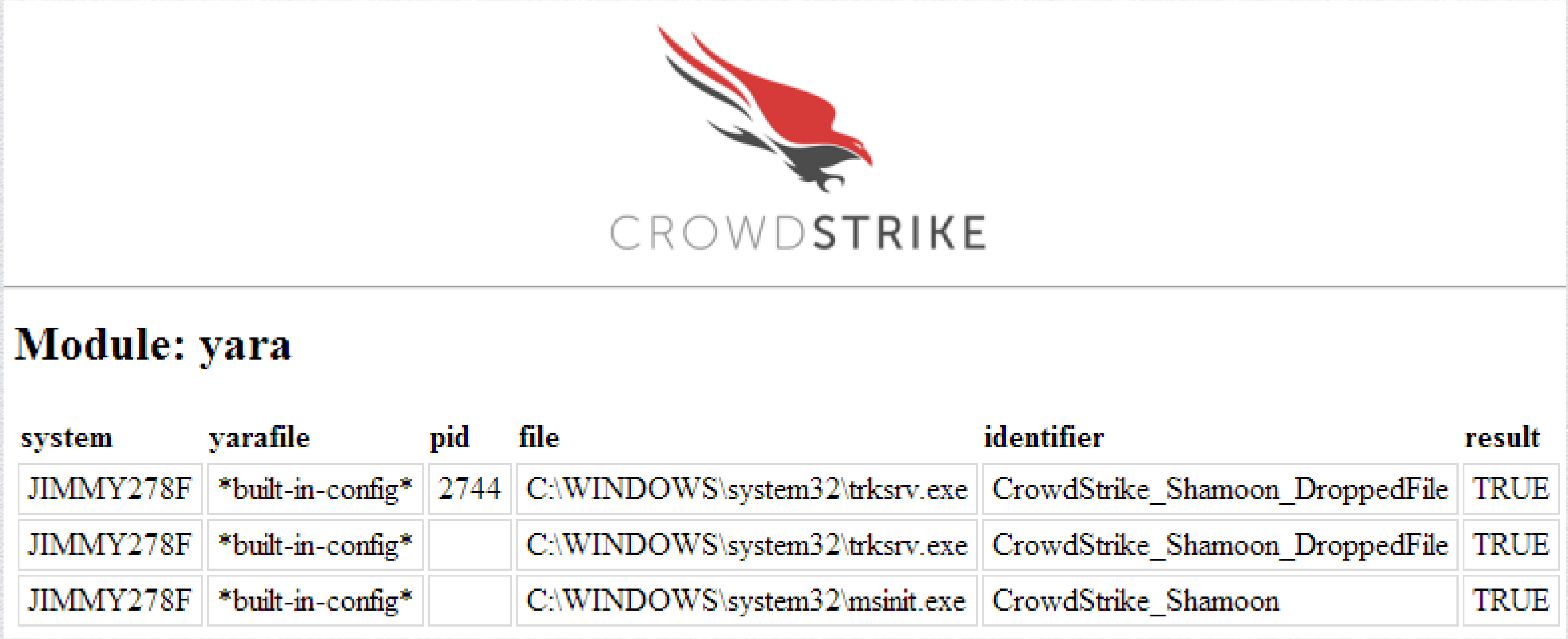
```
rule CrowdStrike_Shamoon_DroppedFile

{   meta:

    description = "Rule to detect Shamoon malware."

    strings:

        $testn123 = "test123" wide

        $testn456 = "test456" wide

        $testn789 = "test789" wide

        $testdomain = "testdomain.com" wide

        $pingcmd = "ping -n 30 127.0.0.1 >nul" wide

    condition:

        (any of ($testn*) or $pingcmd) and $testdomain

}
```



```
Scanning file "C:\WINDOWS\system32\USER32.dll"
Scanning file "C:\WINDOWS\system32\GDI32.dll"
Scanning file "C:\WINDOWS\system32\MSCTF.dll"
Scanning file "C:\WINDOWS\system32\MSUTB.dll"
Scanning file "C:\WINDOWS\system32\IMM32.DLL"
Scanning file "C:\WINDOWS\system32\uxtheme.dll"
Scanning file "C:\WINDOWS\system32\apphelp.dll"
Scanning file "C:\WINDOWS\system32\msctfime.ime"
Scanning file "C:\WINDOWS\system32\ole32.dll"
Scanning file "C:\WINDOWS\system32\shlwapi.dll"
Scanning file "C:\WINDOWS\system32\USERENV.dll"
Scanning file "C:\WINDOWS\system32\trksrv.exe"
  "CrowdStrike_Shamoon_DroppedFile": TRUE
Scanning PID 788 (trksrv.exe)
  "CrowdStrike_Shamoon_DroppedFile": TRUE
Scanning file "C:\WINDOWS\system32\ntdll.dll"
Scanning file "C:\WINDOWS\system32\kernel32.dll"
Scanning file "C:\WINDOWS\system32\NETAPI32.dll"
Scanning file "C:\WINDOWS\system32\msvcrt.dll"
Scanning file "C:\WINDOWS\system32\ADVAPI32.dll"
Scanning file "C:\WINDOWS\system32\RPCRT4.dll"
Scanning file "C:\WINDOWS\system32\Secur32.dll"
Scanning file "C:\WINDOWS\system32\WS2_32.dll"
Scanning file "C:\WINDOWS\system32\WS2HELP.dll"
Scanning file "C:\WINDOWS\system32\USER32.dll"
```

Demo #4

CrowdResponse Reporting



CROWDSTRIKE

Module: yara

system	yarafile	pid	file	identifier	result
JIMMY278F	*built-in-config*	2744	C:\WINDOWS\system32\trksrv.exe	CrowdStrike_Shamoon_DroppedFile	TRUE
JIMMY278F	*built-in-config*		C:\WINDOWS\system32\trksrv.exe	CrowdStrike_Shamoon_DroppedFile	TRUE
JIMMY278F	*built-in-config*		C:\WINDOWS\system32\msinit.exe	CrowdStrike_Shamoon	TRUE

CrowdResponse Community Rules

- Initial release to come with rules for Deep Panda and Energetic Bear actors
- Additional rules to be released periodically by CrowdStrike
- Encourage community rule-sharing

Conclusion

- We are entering in a new era of Targeted Destructive Attacks
  - Moving from data exfiltration to data / system destruction
- Hacktivists will move from DDOS to system destruction
- Imperative to look for adversary activity that will precede destructive activity
- CrowdResponse can be used to look for adversary activity that may be indicative of a multitude of attacks
- Firmware signing for all updates are critical

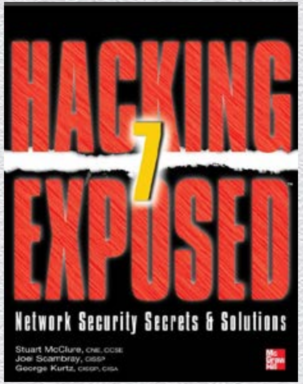
Follow Us

- George Kurtz
  - @George_Kurtz
- Dmitri Alperovitch
  - @DmitriCyber
- Alex Ionescu
  - @aionescu

Additional Resources

Webcasts, Updates, Community Tools
www.hackingexposed7.com

Book Signing at
Veracode Booth #3521
Wed 2/26 - 3pm-4pm


HACKING
7
EXPOSED
Network Security Secrets & Solutions
Stuart McClure, CNE, CCSE
Joel Scambray, CISSP
George Kurtz, CISSP, CISA
Mc Graw Hill