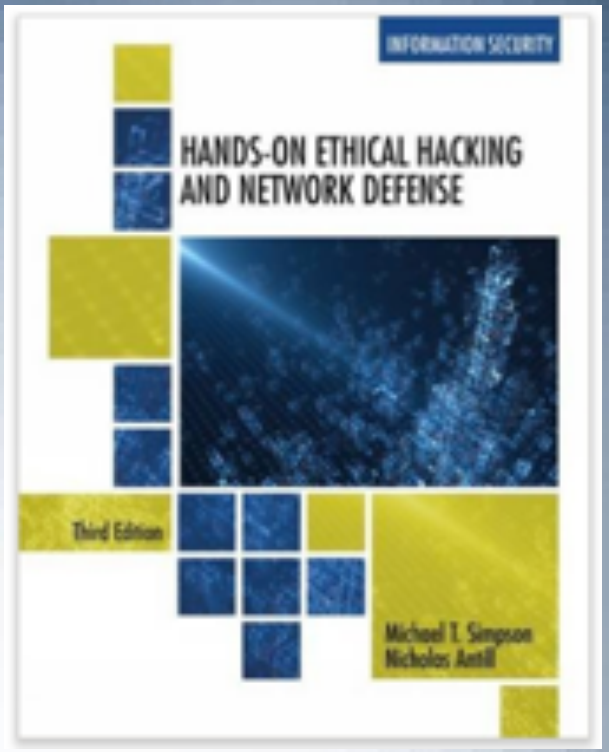
Hands-On Ethical Hacking and Network Defense 3rd Edition



Chapter 8

Desktop and Server OS Vulnerabilities

Last updated 10-25-17

Objectives

- After reading this chapter and completing the exercises, you will be able to:
  - Describe vulnerabilities of Windows and Linux operating systems
  - Identify specific vulnerabilities and explain ways to fix them
  - Explain techniques to harden systems against Windows and Linux vulnerabilities

Windows OS Vulnerabilities

Windows OS Vulnerabilities

- Many Windows OSs have serious vulnerabilities
  - Windows 2000 and earlier
    - Administrators must disable, reconfigure, or uninstall services and features
  - Windows XP, Vista, 7, 8, and 10
    - And Windows Server 2003, 2008, 2012, and 2016;
    - Most services and features are disabled by default

CVE List

- Link Ch 8zk

Search Results

There are **598** CVE entries that match your search.

Name	Description
CVE-2016-3375	The OLE Automation mechanism and VBScript scripting engine in Microsoft Internet Explorer 9 through 11, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."
CVE-2016-3374	The PDF library in Microsoft Edge, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information via a crafted web site, aka "PDF Library Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3370.
CVE-2016-3373	The kernel API in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 does not properly implement registry access control, which allows local users to obtain sensitive account information via a crafted application, aka "Windows Kernel Elevation of Privilege Vulnerability."

Windows File Systems

- File system
  - Stores and manages information
    - User created
    - OS files needed to boot
  - Most vital part of any OS
    - Can be a vulnerability

File Allocation Table

- Original Microsoft file system
  - Supported by nearly all desktop and server OS's
  - Standard file system for most removable media
    - Other than CDs and DVDs
  - Later versions provide for larger file and disk sizes
- Most serious shortcoming
  - Doesn't support file-level access control lists (ACLs)
    - Necessary for setting permissions on files
    - Multiuser environment use results in vulnerability

NTFS

- New Technology File System (NTFS)
  - First released as high-end file system
    - Added support for larger files, disk volumes, and ACL file security
- Subsequent Windows versions
  - Included upgrades for compression, journaling, file-level encryption, and self-healing
- Alternate data streams (ADSs)
  - Can “stream” (hide) information behind existing files
    - Without affecting function, size, or other information
  - Several detection methods

ADS Demo

Administrator: Command Prompt

```
C:\Users\Sam\demo>dir
 Volume in drive C is Win7RTM
 Volume Serial Number is C2E4-15E3

 Directory of C:\Users\Sam\demo

10/05/2010  05:26 AM    <DIR>          .
10/05/2010  05:26 AM    <DIR>          ..
10/05/2010  05:26 AM                 6 foo
               1 File(s)              6 bytes
               2 Dir(s)  12,124,221,440 bytes free

C:\Users\Sam\demo>echo BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB>foo:bar

C:\Users\Sam\demo>dir
 Volume in drive C is Win7RTM
 Volume Serial Number is C2E4-15E3

 Directory of C:\Users\Sam\demo

10/05/2010  05:26 AM    <DIR>          .
10/05/2010  05:26 AM    <DIR>          ..
10/05/2010  05:26 AM                 6 foo
               1 File(s)              6 bytes
               2 Dir(s)  12,124,221,440 bytes free
```

```
C:\Users\Sam\demo>dir /r
 Volume in drive C is Win7RTM
 Volume Serial Number is C2E4-15E3

 Directory of C:\Users\Sam\demo

10/05/2010  05:26 AM    <DIR>          .
10/05/2010  05:26 AM    <DIR>          ..
10/05/2010  05:26 AM                 6 foo
                                    31 foo:bar:$DATA
               1 File(s)              6 bytes
               2 Dir(s)  12,119,650,304 bytes free
```

Remote Procedure Call

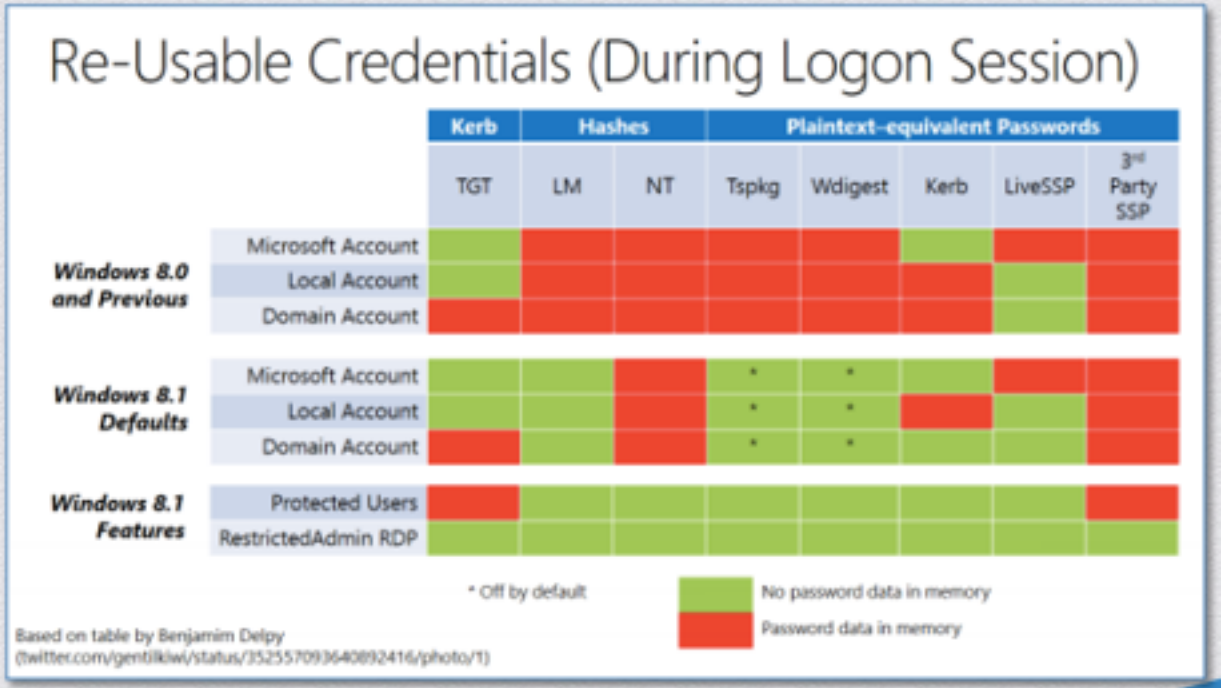
- Interprocess communication mechanism
  - Allows a program running on one host to run code on a remote host
- Worm that exploited RPC
  - Conficker worm
- Microsoft Baseline Security Analyzer
  - Determines if system is vulnerable due to an RPC-related issue

Pass The Hash

Credential Re-Use (link Ch 8zh)

Domain Account Mitigations

- Reduced credential footprint
- Aggressive session expiry
- New “Protected Users” RID
- Hardened LSASS process



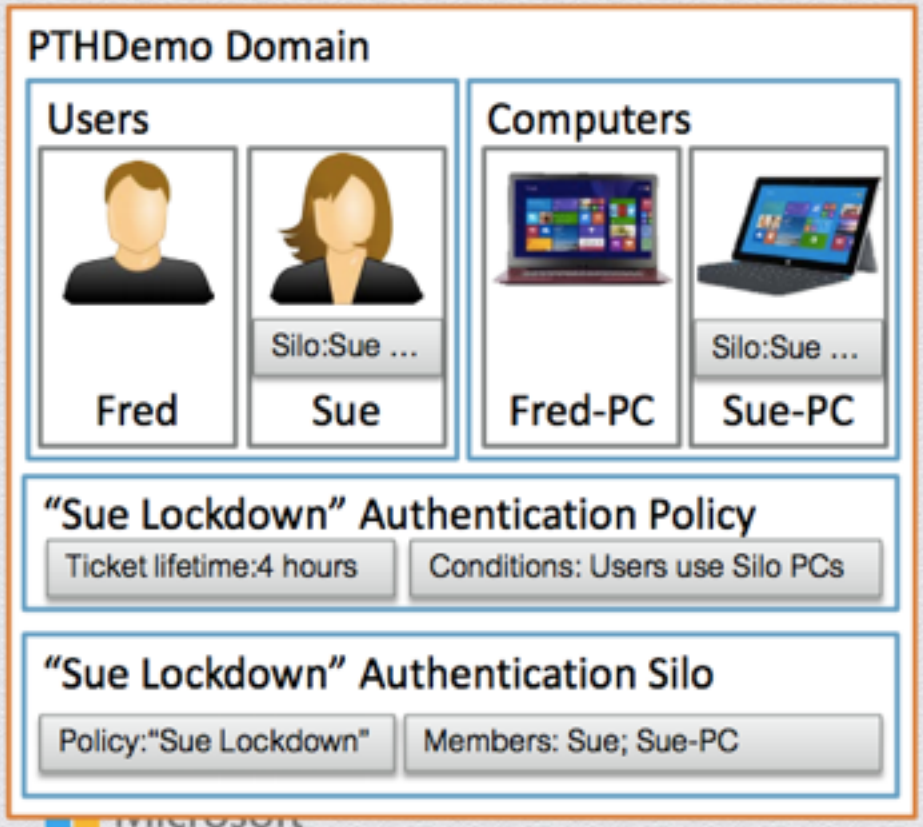
Microsoft

#RSAC

RSACONFERENCE2014

Silos (link Ch 8zh)

Authentication Policies and Silos

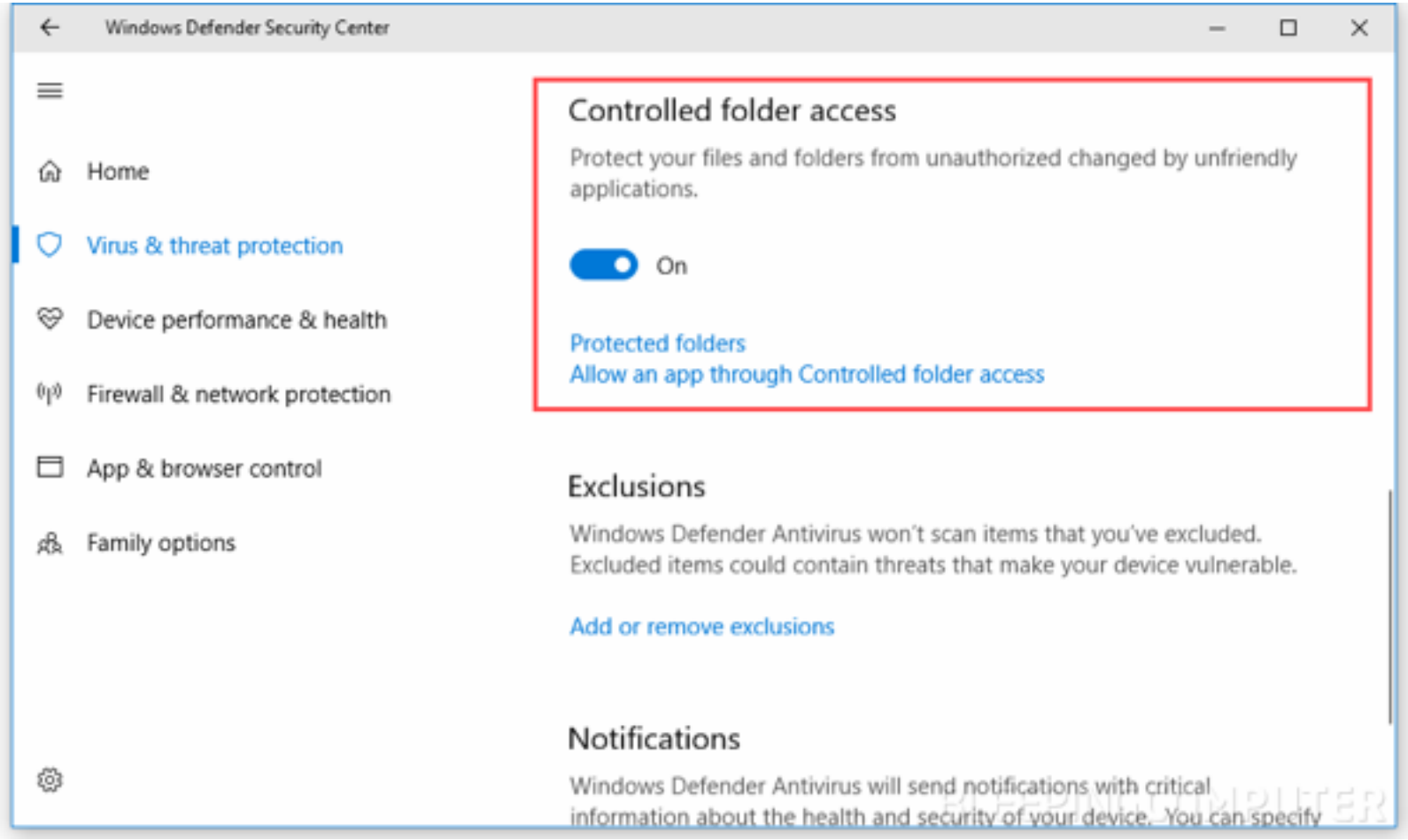


- Enable isolation of users or resources
  - Keeps user in their silo
  - Prevents outside access to silo
- 2012R2 domains support Authentication Policies and Silos
  - Policies allow custom ticket lifetime and issuance conditions
  - Can restrict users and service accounts

Windows Defender Exploit Guard

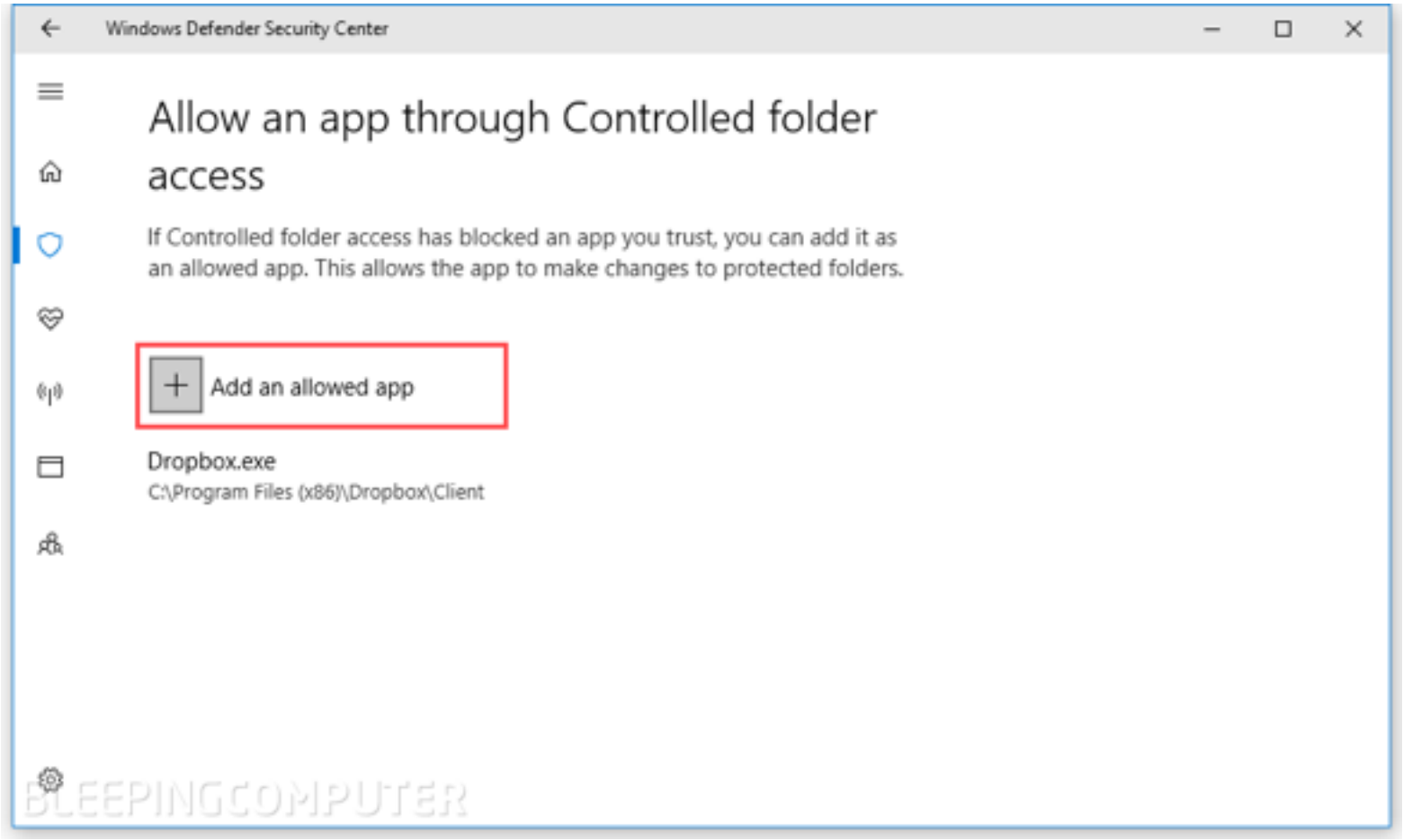
- New in Windows 10 Fall Creators Update (10-23-17)
- **Attack Surface Reduction (ASR)**
  - Uses machine learning to stop zero-day attacks
- **Network protection**
  - Blocks outbound connections to known malicious servers
- **Controlled folder access**
- **Exploit protection**

Controlled Folder Access

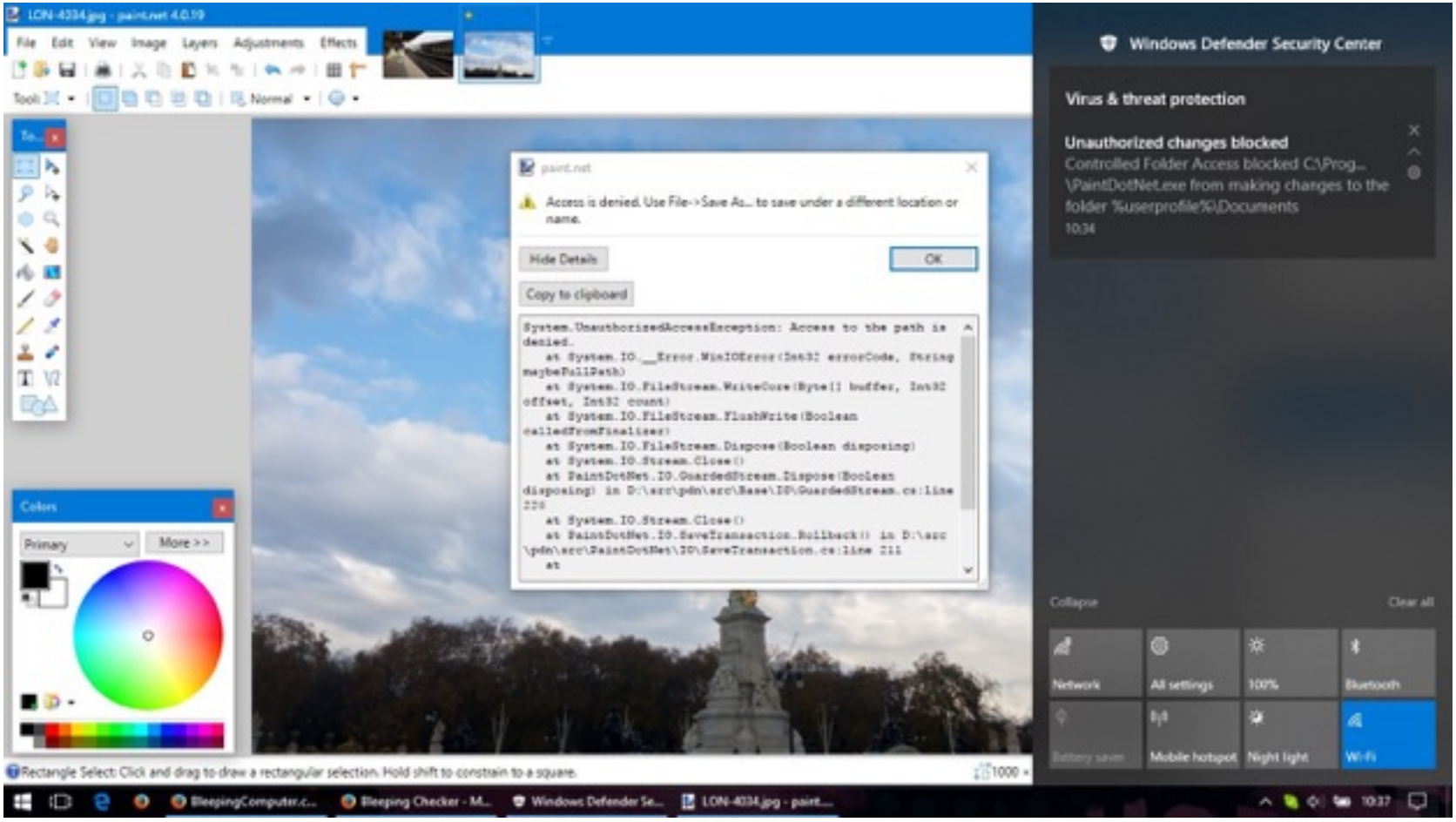


Controlled Folder Access

Controlled Folder Access



Controlled Folder Access



NetBIOS

- Software loaded into memory
  - Enables computer program to interact with network resource or device
- NetBIOS isn’t a protocol
  - Interface to a network protocol
- NetBios Extended User Interface (NetBEUI)
  - Fast, efficient network protocol
  - Allows NetBIOS packets to be transmitted over TCP/IP
  - NBT is NetBIOS over TCP

NetBIOS (cont'd.)

- Systems running newer Windows OSs
  - Vista, Server 2008, Windows 7, and later versions
  - Share files and resources without using NetBIOS
- NetBIOS is still used for backward compatibility
  - Companies use old machines

Server Message Block

- Used to share files
  - Usually runs on top of:
    - NetBIOS
    - NetBEUI, or
    - TCP/IP
- Several hacking tools target SMB
  - L0phtcrack's SMB Packet Capture utility and SMBRelay
    - It took Microsoft seven years to patch these

Server Message Block (cont'd.)

- SMB2
  - Introduced in Windows Vista
  - Several new features
  - Faster and more efficient
- Windows 7
  - Microsoft avoided reusing code
  - Still allowed backward capability
    - Windows XP Mode
  - Spectacular DoS vulnerabilities
    - Links Ch 8za-8zc

Laurent Gaffié's Fuzzer

- Look how easy it is!
- From Link Ch 8zb

So I hardcoded a pretty simple fuzzer (python) for this approach:

```
from socket import *
from time import sleep
from random import choice

host = "IP_ADDR", 445

#Negotiate Protocol Request
packet = [chr(int(a, 16)) for a in """
00 00 00 90
ff 53 4d 42 72 00 00 00 00 18 53 c8 00 00 00 00
00 00 00 00 00 00 00 00 ff ff ff fe 00 00 00 00
00 6d 00 02 50 43 20 4e 45 54 57 4f 52 4b 20 50
52 4f 47 52 41 4d 20 31 2e 30 00 02 4c 41 4e 4d
41 4e 31 2e 30 00 02 57 69 6e 64 6f 77 73 20 66
6f 72 20 57 6f 72 6b 67 72 6f 75 70 73 20 33 2e
31 61 00 02 4c 4d 31 2e 32 58 30 30 32 00 02 4c
41 4e 4d 41 4e 32 2e 31 00 02 4e 54 20 4c 4d 20
30 2e 31 32 00 02 53 4d 42 20 32 2e 30 30 32 00
""".split()]


while True:
#/Core#
what = packet[:]
where = choice(range(len(packet)))
which = chr(choice(range(256)))
what[where] = which
#/Core#
#sending stuff @host
sock = socket()
sock.connect(host)
sock.send(''.join(what))
sleep(0.1) # dont flood it
print 'fuzzing param %s' % (which.encode("hex"))
print 'complete packet %s' % (''.join(what).encode("hex"))
# When SMB Or RPC die (with TCP), sock get a timed out and die
@the last packet, printing these things is more than usefull
sock.close()
```

This simple fuzzer pwned smb2 in 3 seconds.

Common Internet File System

- Standard protocol
  - Replaced SMB for Windows 2000 Server and later
  - SMB is still used for backward compatibility
  - Described as just a renaming of SMB by Wikipedia (link Ch 8z)
- Remote file system protocol
  - Enables sharing of network resources over the Internet
- Relies on other protocols to handle service announcements
  - Notifies users of available resources

Common Internet File System (cont'd.)

- Enhancements
  - Locking features
  - Caching and read-ahead/write-behind
  - Support for fault tolerance
  - Capability to run more efficiently over dial-up
  - Support for anonymous and authenticated access
- Server security methods
  - Share-level security (folder password)
  - User-level security (username and password)

Common Internet File System (cont'd.)

- Attackers look for servers designated as domain controllers
  - Severs handle authentication
- Windows Server 2003 and 2008
  - Domain controller uses a global catalog (GC) server
    - Locates resources among many objects

Domain Controller Ports

- By default, Windows Server 2003 and 2008 domain controllers using CIFS listen on the following ports
  - DNS (port 53)
  - HTTP (port 80)
  - Kerberos (port 88)
  - RPC (port 135)
  - NetBIOS Name Service (port 137)
  - NetBIOS Datagram Service (port 139)
  - LDAP (port 389)
  - HTTPS (port 443)
  - SMB/ CIFS (port 445)
  - LDAP over SSL (port 636)
  - Active Directory global catalog (port 3268)

Null Sessions

- Anonymous connection established without credentials
  - Used to display information about users, groups, shares, and password policies
  - Necessary only if networks need to support older Windows versions
- To enumerate NetBIOS vulnerabilities use:
  - Nbtstat, Net view, Netstat, Ping, Pathping, and Telnet commands

Web Services

- IIS installs with critical security vulnerabilities
  - IIS Lockdown Wizard
    - Locks down IIS versions 4.0 and 5.0
- IIS 6.0 and later versions
  - Installs with a “secure by default” mode
  - Previous versions left crucial security holes
- Keeping a system patched is important
- Configure only needed services

SQL Server

- Many potential vulnerabilities
  - Null System Administrator (SA) password
    - SA access through SA account
    - SA with blank password by default on versions prior to SQL Server 2005
  - Gives attackers administrative access
    - Database and database server

Buffer Overflows

- Data is written to a buffer and corrupts data in memory next to allocated buffer
  - Normally, occurs when copying strings of characters from one buffer to another
- Functions don't verify text fits
  - Attackers run shell code
- C and C++
  - Lack built-in protection against overwriting data in memory

Passwords and Authentication

- Weakest security link in any network
  - Authorized users
    - Most difficult to secure
    - Relies on people
  - Companies should take steps to address it

Passwords and Authentication (cont'd.)

- Comprehensive password policy is critical
  - Should include:
    - Change passwords regularly
    - Require at least six characters **(too short!)**
    - Require complex passwords
    - Passwords can't be common words, dictionary words, slang, jargon, or dialect
    - Passwords must not be identified with a user
    - Never write it down or store it online or in a file
    - Do not reveal it to anyone
    - Use caution when logging on and limit reuse

Passwords and Authentication (cont'd.)

- Configure domain controllers
  - Enforce password age, length, and complexity
- Password policy aspects that can be enforced:
  - Account lockout threshold
    - Set number of failed attempts before account is disabled temporarily
  - Account lockout duration
    - Set period of time account is locked out after failed logon attempts
- Disable LM Hashes


Kahoot!

Tools for Identifying Vulnerabilities in Windows

Tools for Identifying Vulnerabilities in Windows

- Many tools are available
  - Using more than one is advisable
- Using several tools
  - Helps pinpoint problems more accurately

Built-in Windows Tools

- Microsoft Baseline Security Analyzer (MBSA)
  - Capable of checking for:
    - Patches
    - Security updates
    - Configuration errors
    - Blank or weak passwords

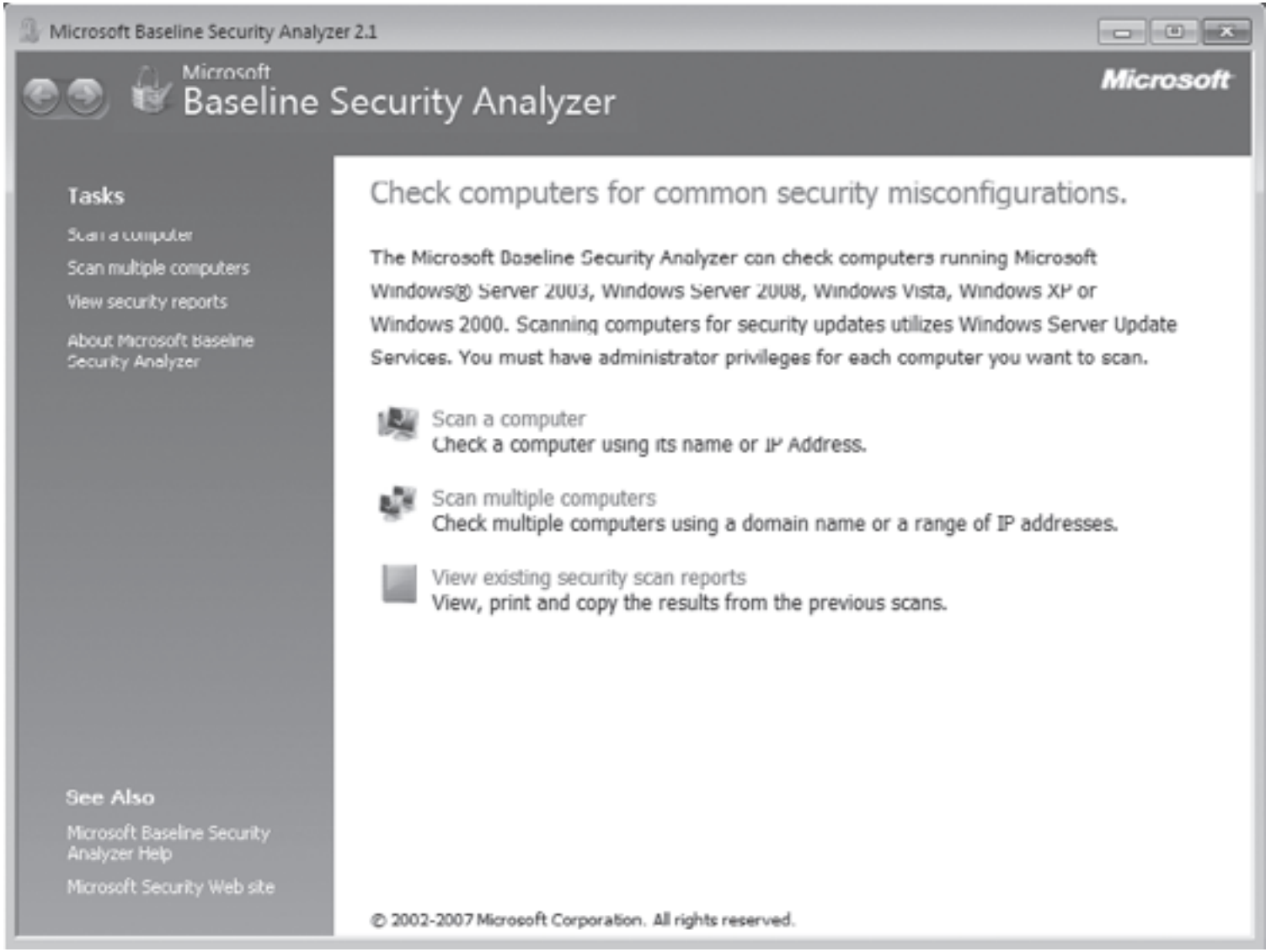


Figure 8-1 Checks available in MBSA

Type of check	Checks for:
Security update checks	Missing Windows, IIS, and SQL Server security updates Missing Exchange Server security updates Missing IE security updates Missing Windows Media Player and Office security updates Missing Microsoft Virtual Machine (VM) and Microsoft Data Access Components (MDAC) security updates Missing MSXML and Content Management Server security updates
Windows checks	Account password expiration and whether blank or simple passwords are used for local user accounts File system type on hard drives Whether the Auto Logon feature is enabled Whether the Guest account is enabled and the number of local Administrator accounts RestrictAnonymous Registry key setting List shares on the computer and any unnecessary services running Windows version and whether Windows auditing is enabled Firewall status and Automatic Updates status

Table 8-2 Checks performed by MBSA in full-scan mode

Type of check	Checks for:
IIS checks	Whether the IIS Lockdown tool is running Whether IIS sample applications and the IIS Admin virtual folder are installed Whether IIS parent paths are enabled Whether MSADC and Scripts virtual directories are installed Whether IIS logging is enabled Whether IIS is running on a domain controller
SQL checks	Whether the Administrators group belongs in the Sysadmin role and whether the CmdExec role is restricted to Sysadmin only Whether SQL Server is running on a domain controller Whether the SA account password is exposed and the Guest account has database access Access permissions to SQL Server installation folders Whether the Everyone group has access to SQL Server Registry keys Whether SQL Server service accounts are members of the local Administrators group Whether SQL Server accounts have blank or simple passwords SQL Server authentication mode type and number of Sysadmin role members
Desktop application checks	IE security zone settings for each local user Whether IE Enhanced Security Configuration is enabled for Administrator accounts Whether IE Enhanced Security Configuration is enabled for non-Administrator accounts Microsoft Office security zone settings for each local user

Table 8-2 Checks performed by MBSA in full-scan mode (cont'd.)

Using MBSA

- System must meet minimum requirements
  - Before installing
- After installing, MBSA can:
  - Scan itself
  - Scan other computers remotely
  - Be scanned remotely

Best Practices for Hardening Windows Systems

Patching Systems

- Best way to keep systems secure
  - Keep up to date
    - Attackers take advantage of known vulnerabilities
- Options for small networks
  - Accessing Windows Update manually
  - Configure Automatic Updates
- Options for large networks from Microsoft
  - Systems Management Server (SMS)
  - Windows Software Update Service (WSUS)
  - SCCM (System Center Configuration Manager)

Patching Systems

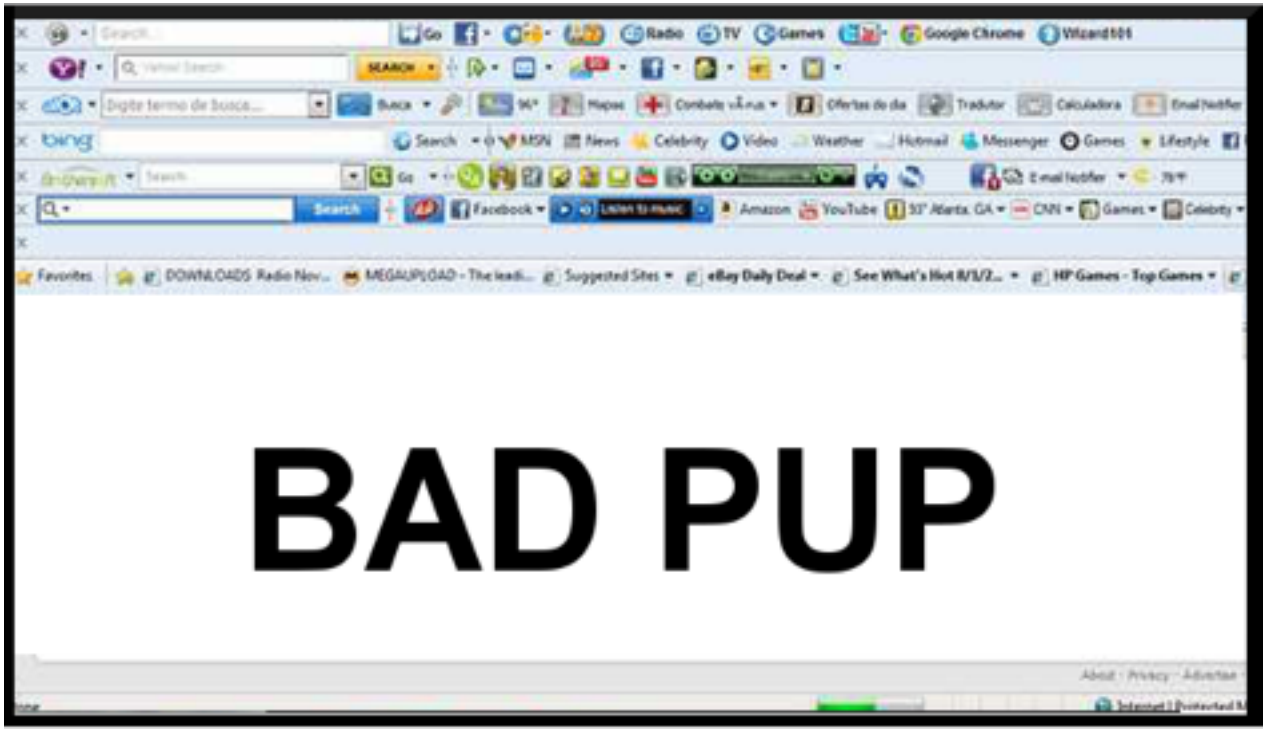
- Third-party patch management solutions
  - BigFix
  - Tanium
  - BladeLogic

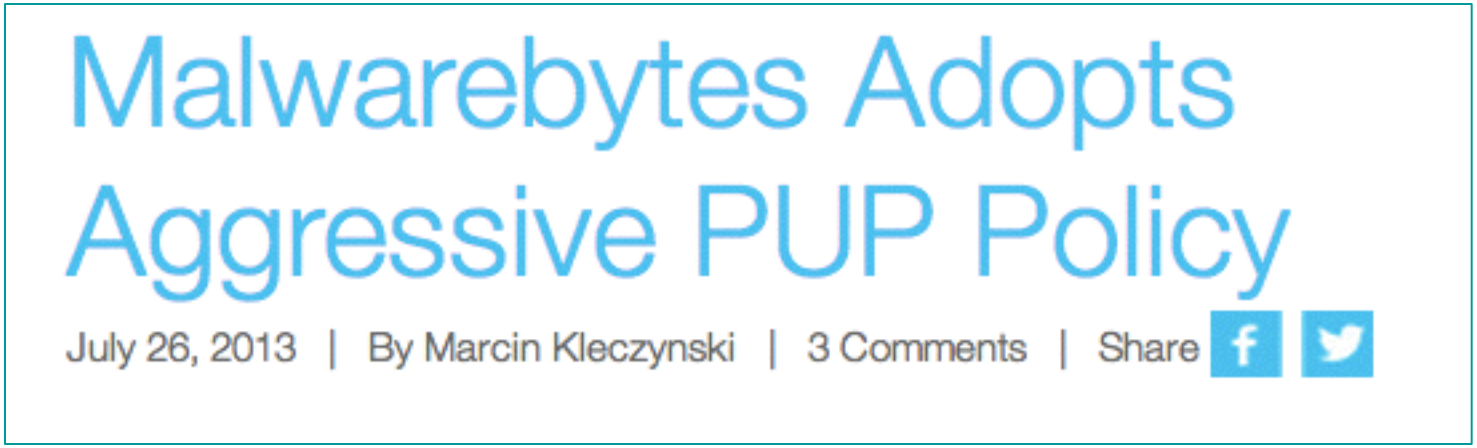
Antivirus Solutions

- Antivirus solution is essential
  - Small networks
    - Desktop antivirus tool with automatic updates
  - Large networks
    - Require corporate-level solution
- Antivirus tools
  - Almost useless if not updated regularly

PUPs (Potentially Unwanted Programs)

- Programs that come bundled with freeware
- Not technically viruses or illegal
- Most antivirus won't block them by default





- Link Ch 8zi, 8zj

Enable Logging and Review Logs Regularly

- Important step for monitoring critical areas
  - Performance
  - Traffic patterns
  - Possible security breaches
- Can have negative impact on performance
- Review regularly
  - Signs of intrusion or problems
    - Use log-monitoring tool

Disable Unused Services and Filtering Ports

- Disable unneeded services
- Delete unnecessary applications or scripts
  - Unused applications are invitations for attacks
- Reducing the attack surface
  - Open only what needs to be open, and close everything else
- Filter out unnecessary ports
  - Make sure perimeter routers filter out ports 137 to 139 and 445

Other Security Best Practices

- Other practices include:
  - Limit the number of Administrator accounts
  - Implement software to prevent sensitive data from leaving the network (Data Loss Prevention)
  - Use network segmentation to make it more difficult for an attacker to move from computer to computer
  - Restrict the number of applications allowed to run
  - Delete unused scripts and sample applications
  - Delete default hidden shares

Other Security Best Practices

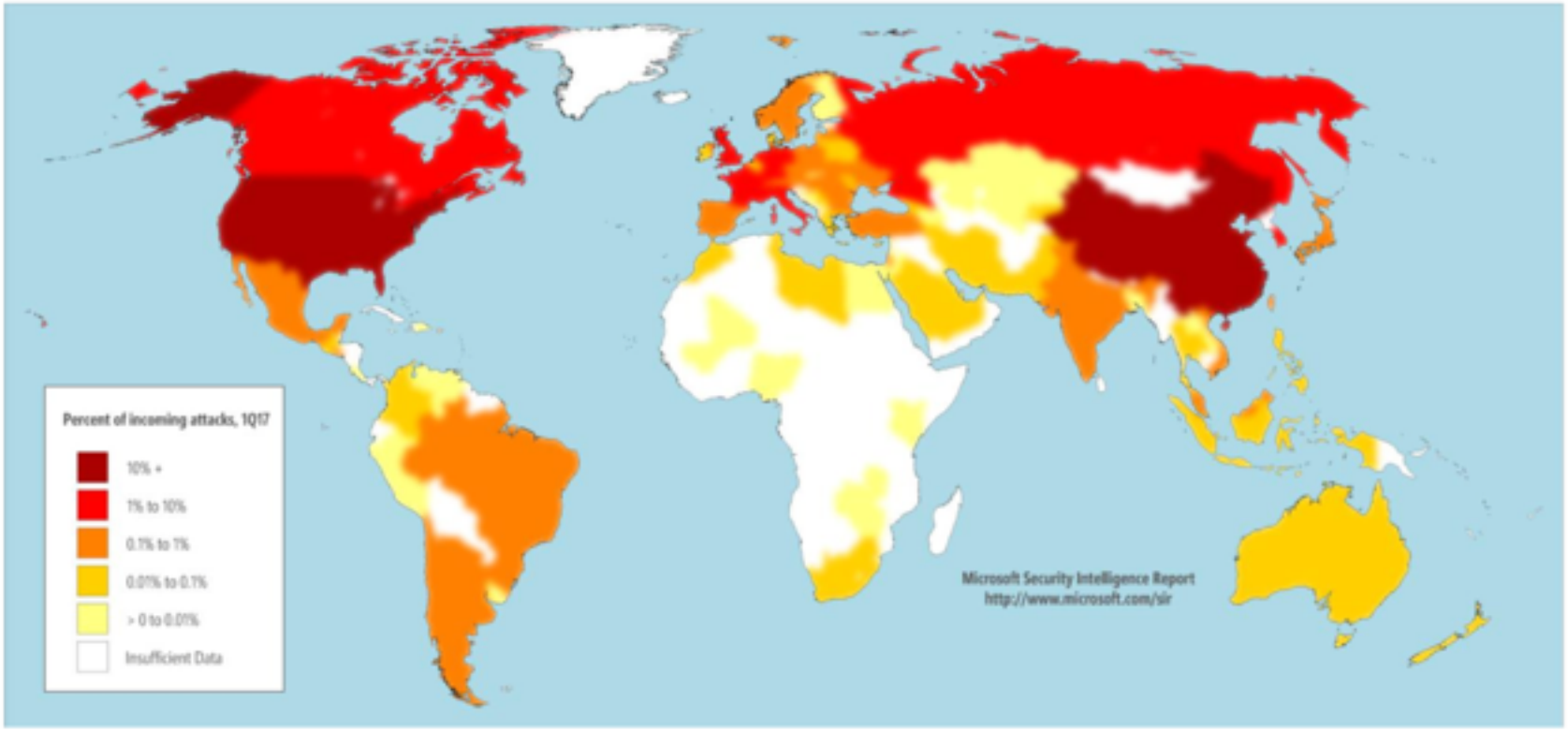
- Other practices include:
  - Use different naming scheme and passwords for public interfaces
  - Ensure sufficient length and complexity of passwords
  - Be careful of default permissions
  - Use appropriate packet-filtering techniques such as firewalls and Intrusion Detection Systems
  - Use available tools to assess system security
  - Use a file integrity checker like Tripwire

Other Security Best Practices (cont'd.)

- Other practices include (cont'd.):
  - Disable Guest account
  - Disable the local Administrator account
  - Make sure there are no accounts with blank passwords
  - Use Windows group policies to enforce security configurations
  - Develop a comprehensive security awareness program
  - Keep up with emerging threats

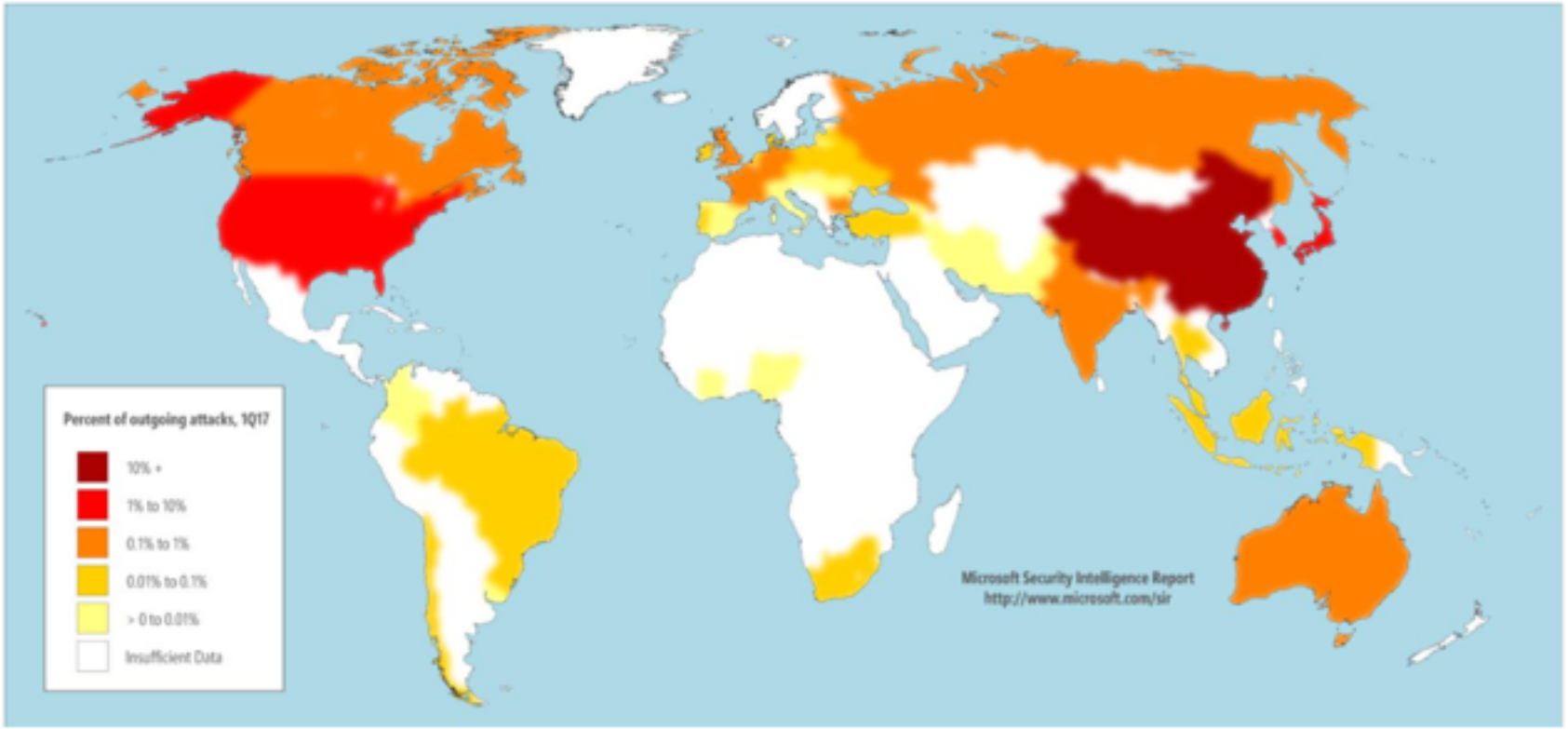

Microsoft Security
Intelligence Report
Volume 22 | January through March, 2017
Microsoft

Figure 4. Incoming attacks detected by Azure Security Center in 1Q17, by country/region of origin



More than two-thirds of incoming attacks on Azure services in 1Q17 came from IP addresses in China and the United States, at 35.1 percent and 32.5 percent, respectively. Korea was third at 3.1 percent, followed by 116 other countries and regions.

Figure 5. Outgoing communication to malicious IP addresses detected by Azure Security Center in 1Q17, by address location



Compromised virtual machines often communicate with command-and-control (C&C) servers at known malicious IP addresses to receive instructions. More than 89 percent of the malicious IP addresses contacted by compromised Azure virtual machines in 1Q17 were located in China, followed by the United States at 4.2 percent.

Bing detected 0.17 drive-by download pages for every 1,000 pages in the index in March 2017.

Figure 9. Monthly trends for countries/regions with the highest concentration of drive-by download pages in March 2017

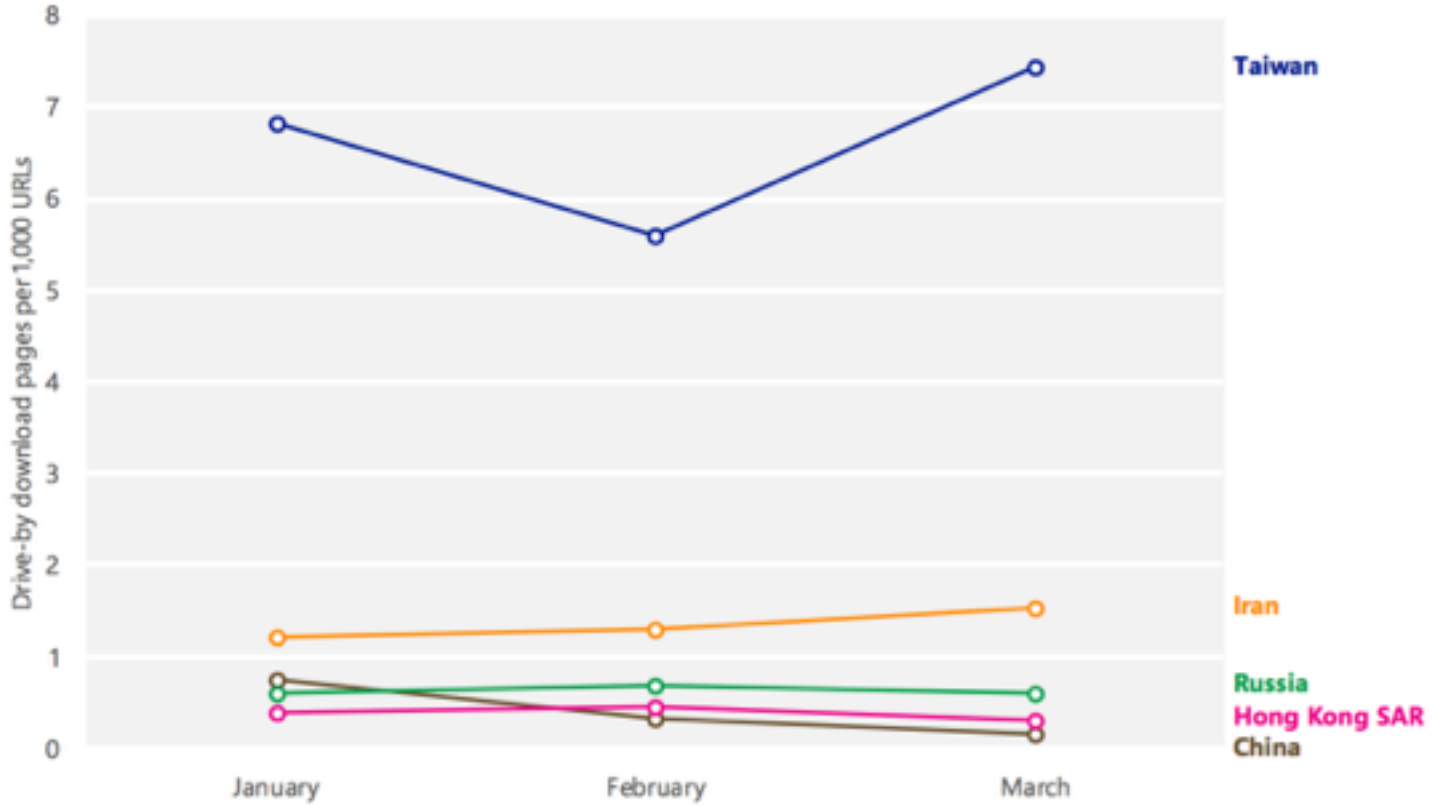


Figure 13. Encounter rates for significant malicious software categories, January–March 2017

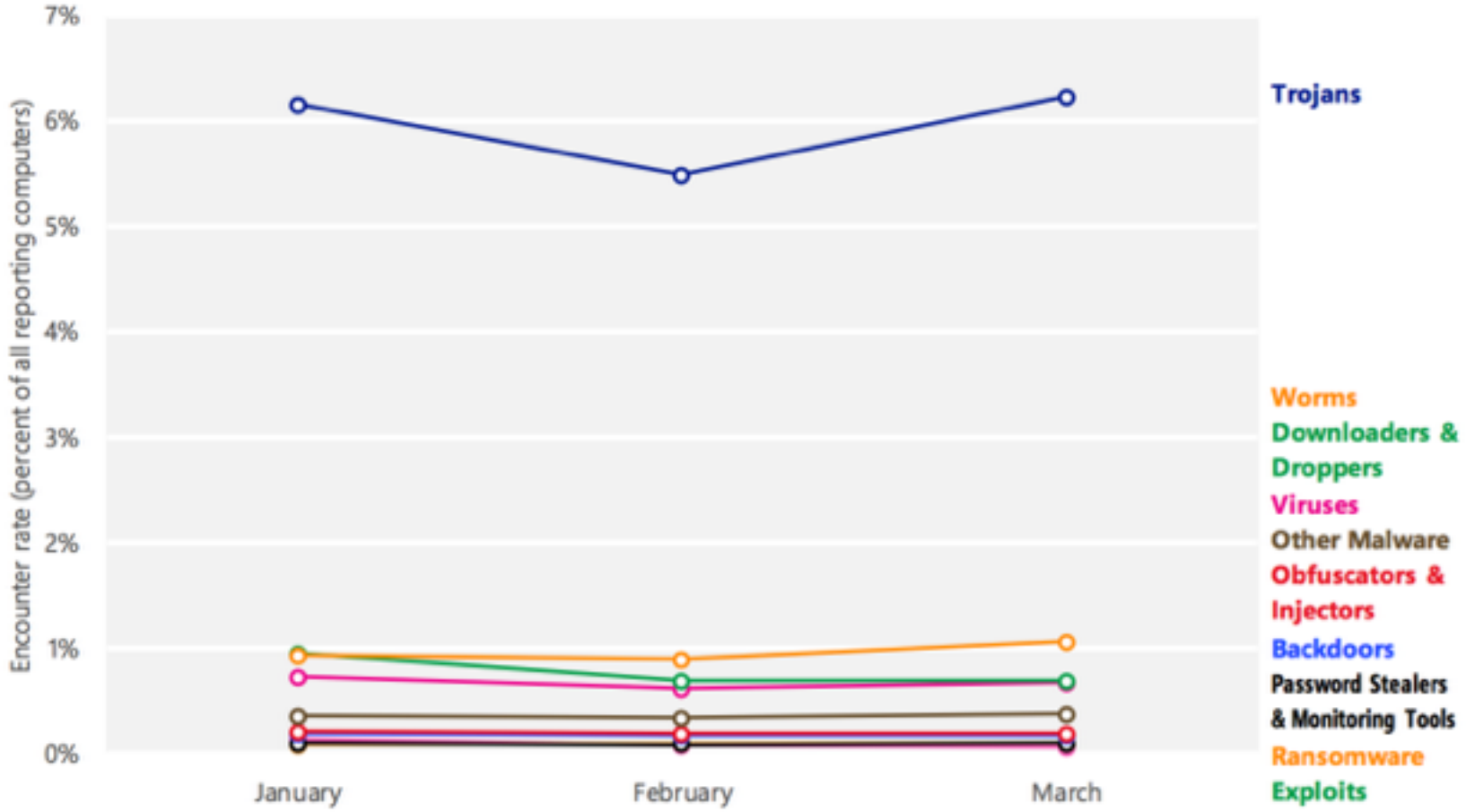


Figure 14. Encounter rates for unwanted software categories, January–March 2017

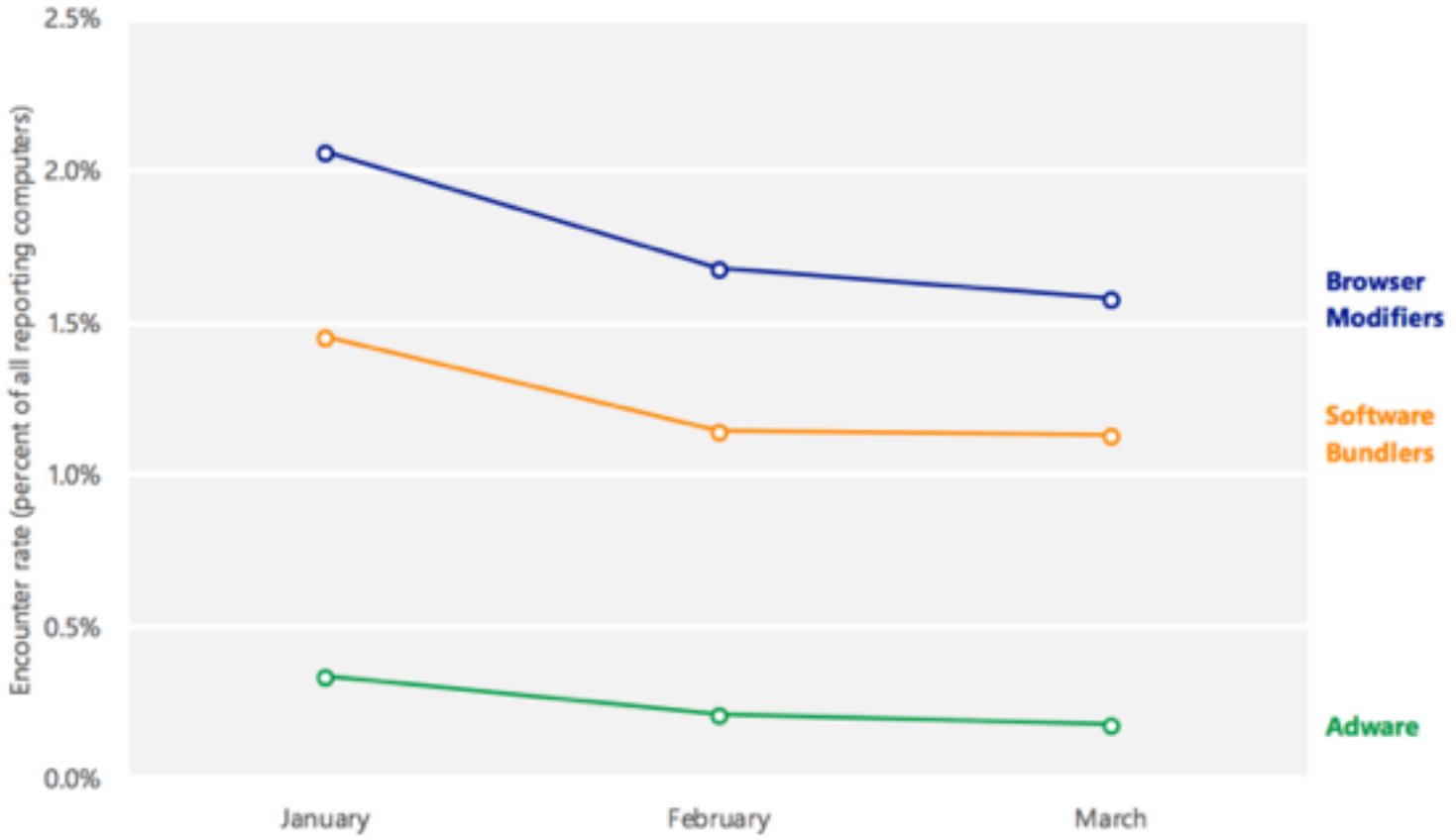
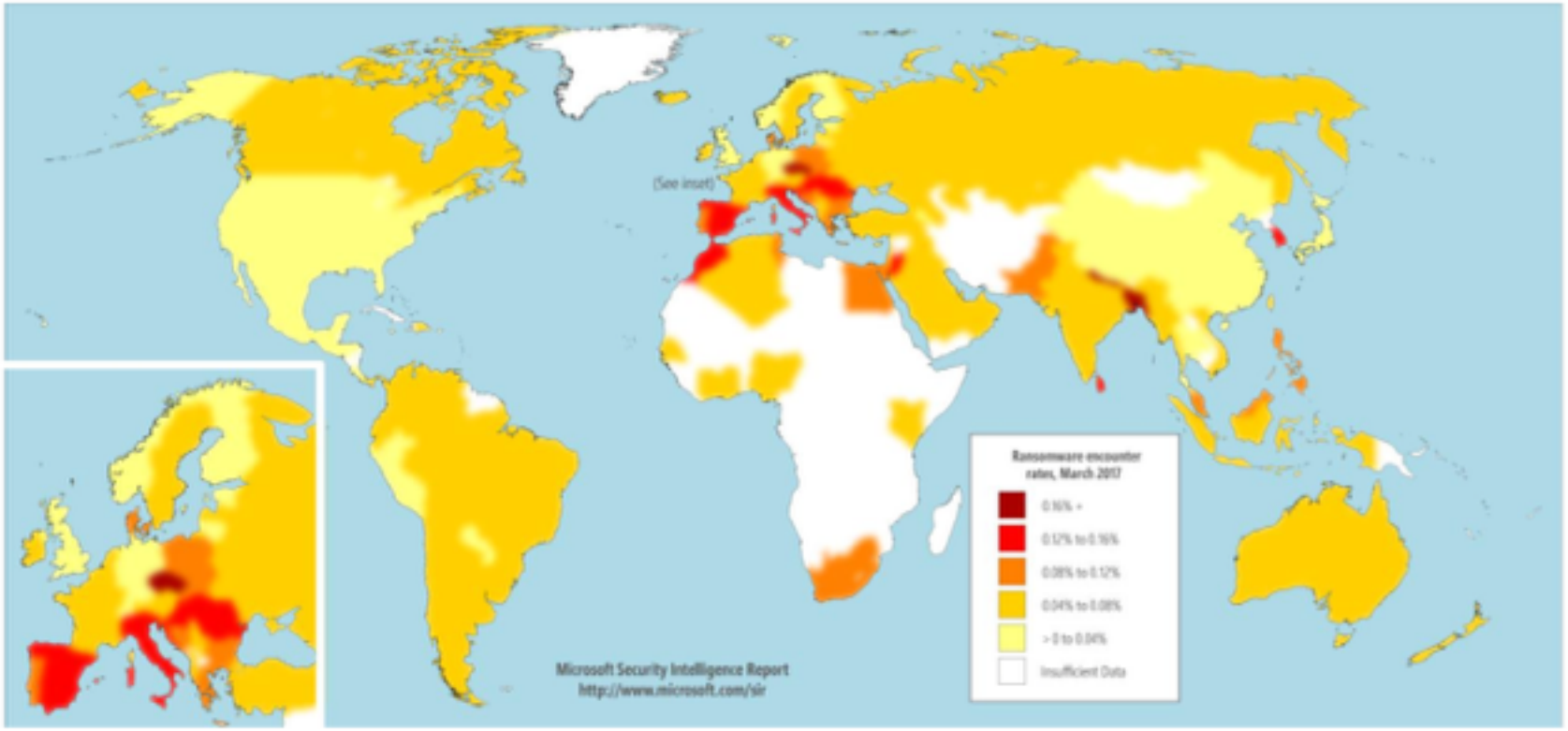


Figure 22. Encounter rates for ransomware families by country/region in March 2017



- Locations with the highest ransomware encounter rates include the Czech Republic (0.17 percent), Korea (0.15 percent), and Italy (0.14 percent).
- Locations with the lowest ransomware encounter rates include Japan (0.012 percent in March 2017), China (0.014 percent), and the United States (0.02 percent).

Linux OS Vulnerabilities

Linux OS Vulnerabilities

- Linux can be made more secure
  - Awareness of vulnerabilities
  - Keep current on new releases and fixes
- Many versions are available
  - Differences ranging from slight to major
- It’s important to understand basics
  - Run control and service configuration
  - Directory structure and file system
  - Basic shell commands and scripting
  - Package management

Samba

- Open-source implementation of CIFS
  - Created in 1992
- Allows sharing resources over a network
  - Security professionals should have basic knowledge of SMB and Samba
    - Many companies have a mixed environment of Windows and *nix systems
- Used to “trick” Windows services into believing *nix resources are Windows resources

Tools for Identifying Linux Vulnerabilities

- CVE Web site
  - Source for discovering possible attacker avenues

CVE/CAN	Description
CVE-2009-1439	A buffer overflow in the Linux kernel's CIFS module allows remote attackers to crash the system by using a specially crafted file-sharing response sent over the network.
CVE-2009-1389	A buffer overflow in a Linux kernel NIC driver allows remote attackers to crash the system by sending a specially crafted large packet.
CVE-2009-0577	An integer overflow in the Common UNIX Printer Daemon (CUPS) on Red Hat Enterprise Linux (RHEL) 3 allows remote attackers to run code and take over the system.

Table 8-4 Linux vulnerabilities found at CVE

Tools for Identifying Linux Vulnerabilities (cont'd.)

- OpenVAS can enumerate multiple OSs
  - Security tester using enumeration tools can:
    - Identify a computer on the network by using port scanning and zone transfers
    - Identify the OS by conducting port scanning
    - Identify via enumeration any logon accounts
    - Learn names of shared folders by using enumeration
    - Identify services running

Checking for Trojan Programs

- Most Trojan programs perform one or more of the following:
  - Allow remote administration of attacked system
  - Create a file server on attacked computer
    - Files can be loaded and downloaded
  - Steal passwords from attacked system
    - E-mail them to attacker
  - Log keystrokes
    - E-mail results or store them in a hidden file the attacker can access remotely
  - Encrypt or destroy files on the system

Checking for Trojan Programs (cont'd.)

- Linux Trojan programs
  - Sometimes disguised as legitimate programs
  - Contain program code that can wipe out file systems
  - More difficult to detect today
    - Protecting against identified Trojan programs is easier
- Rootkits containing Trojan binary programs
  - More dangerous
  - Attackers hide tools
    - Perform further attacks
    - Have access to backdoor programs

More Countermeasures Against Linux Attacks

- Most critical tasks:
  - User awareness training
  - Keeping current
  - Configuring systems to improve security

User Awareness Training

- Inform users
  - No information should be given to outsiders
    - Knowing OS makes attacks easier
  - Be suspicious of people asking questions
    - Verify who they are talking to
    - Call them back

Keeping Current

- As soon as a vulnerability is discovered and posted
  - OS vendors notify customers
    - Upgrades
    - Patches
  - Installing fixes promptly is essential
- Linux distributions
  - Most have warning methods

Secure Configuration

- Many methods to help prevent intrusion
  - Vulnerability scanners
  - Built-in Linux tools
  - SE Linux implements Mandatory Access Control
    - Included in many Linux distributions
  - Free benchmark tools
    - Center for Internet Security
  - Security Blanket

Description: Security Blanket is the only enterprise platform that automatically configures OS's to meet industry standard security requirements. A cost effective way to consistently secure your enterprise in a fraction of the time it takes to lock them manually.


Kahoot!