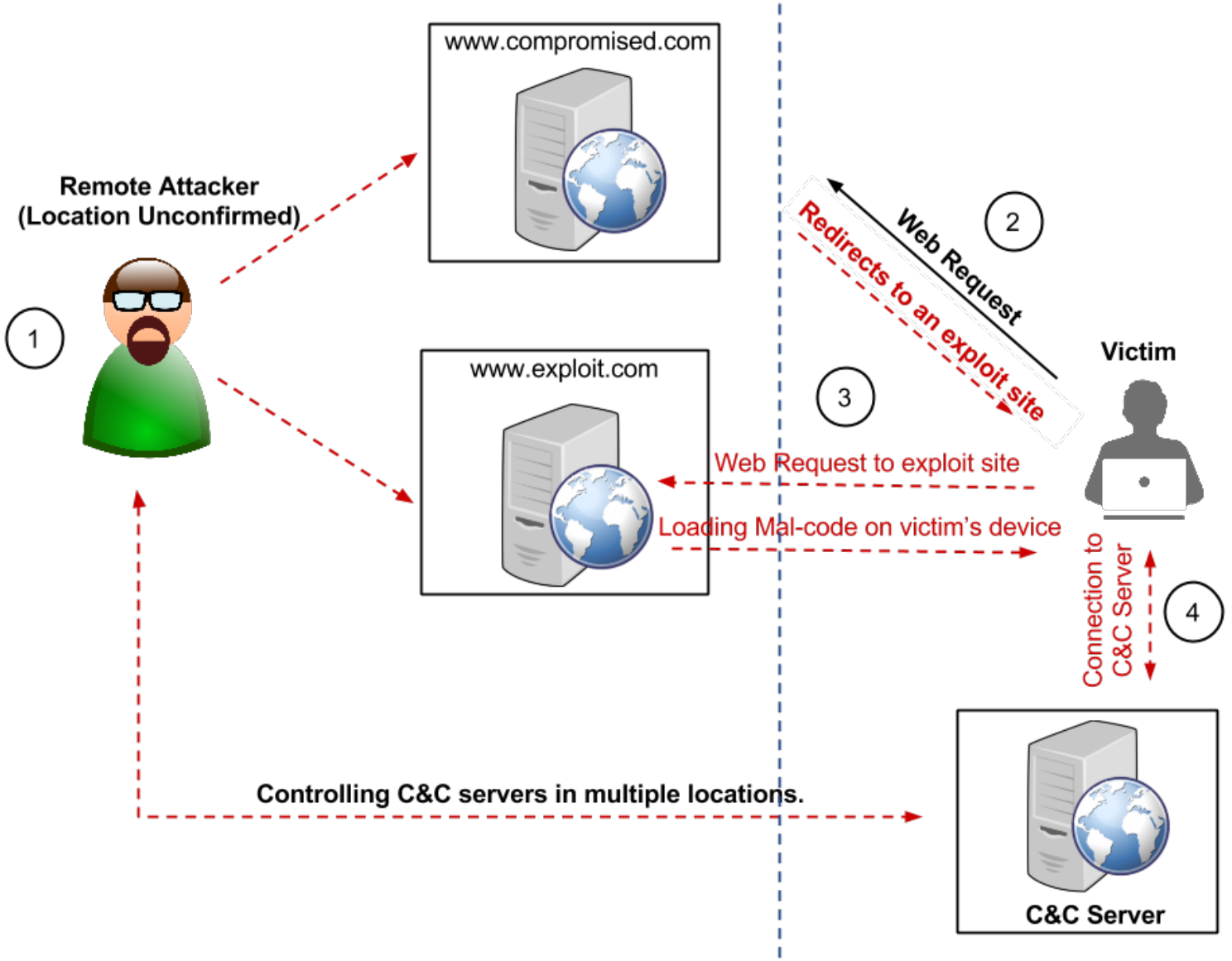
Special Topics in Security
ECE 5698

Engin Kirda
ek@ccs.neu.edu

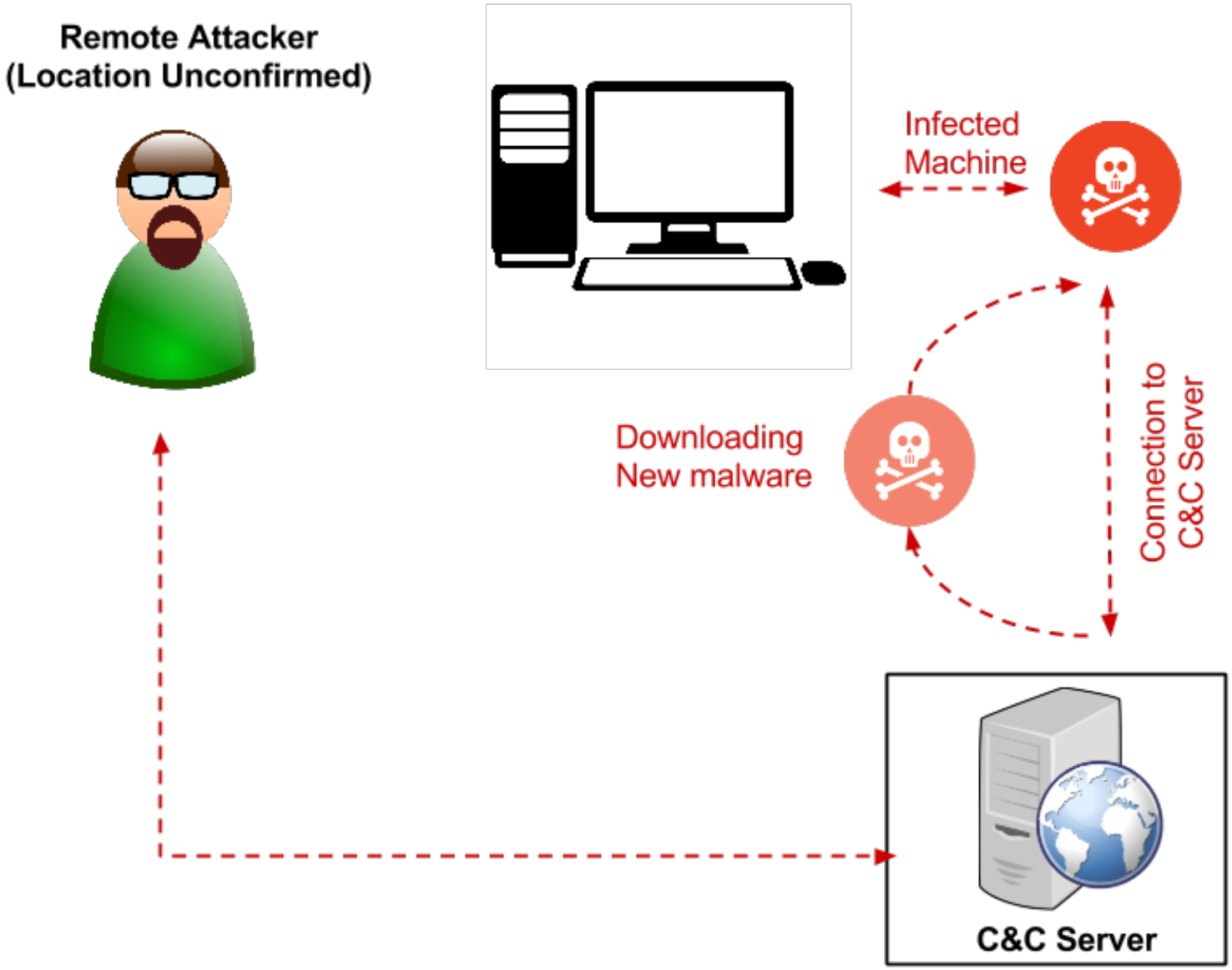
Northeastern University

Malware Attacks

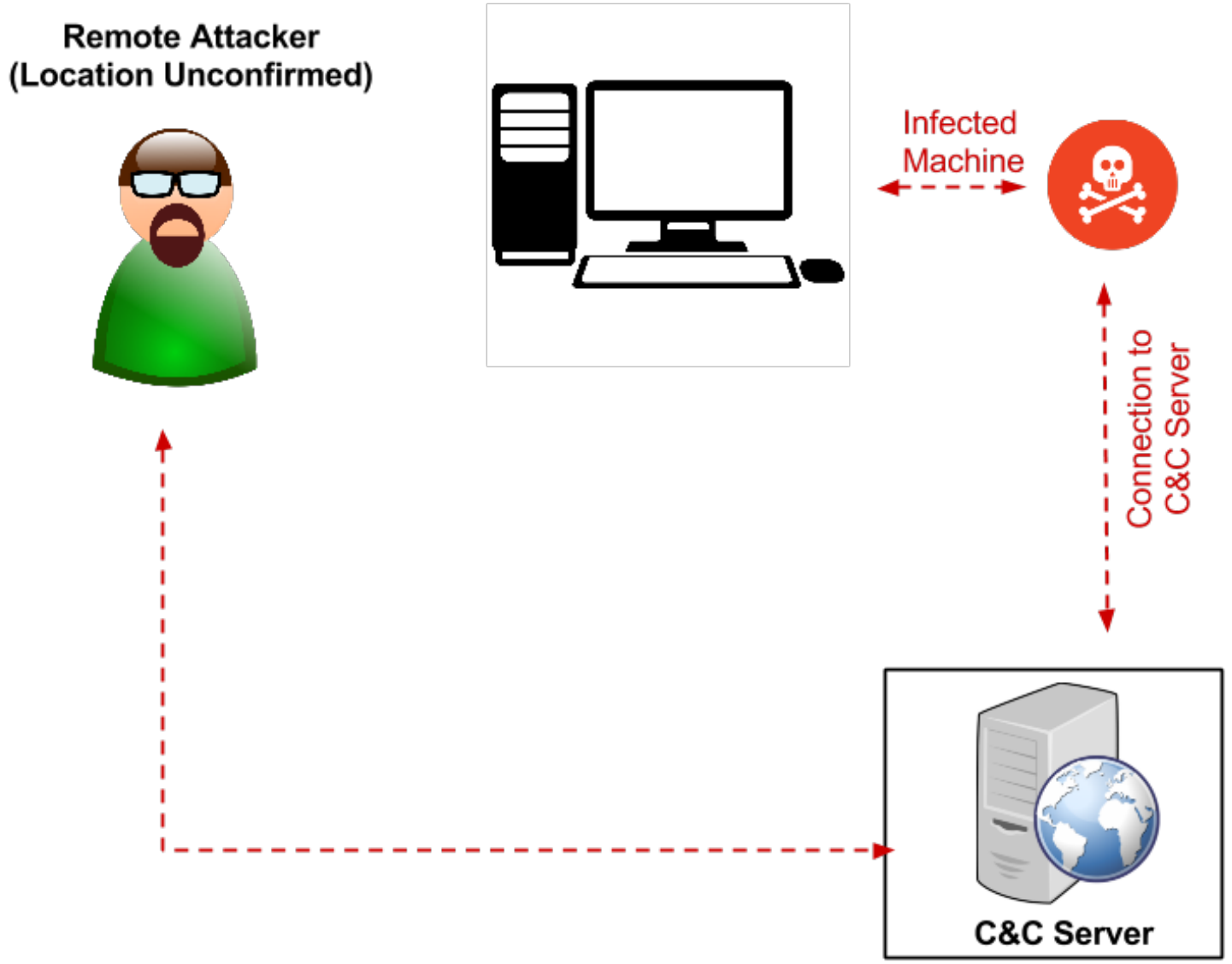
Malware Attacks (Drive-by download attacks)



Malware Attacks (multi-infection)



Maleware Attacks (secure,distributed connection)



Trojan Horses

Trojan Horse

- Trojan horse is a malicious program that is disguised as legitimate software
  - software may look useful or interesting (or at the very least harmless)
  - term derived from the classical myth of the Trojan Horse

- Two types of Trojan horses
  1. malicious functionality is included into useful program
     - disk utility, screensaver, weather alert program
     - famous compiler that generated backdoor into code
  2. malware is stand-alone program
     - possibly disguised file name (sexy.jpg.exe)

Trojan Horse

- Many different types and functions
  - spy on (sensitive) user data
    - log keystrokes, monitor surfing activity
  - disguise presence
    - rootkits
  - allow remote access
    - file transfer, remote program execution
    - base for further attacks, mail relay (for spammers)
    - Back Orifice, NetBus, SubSeven
  - damage routines
    - corrupting files
    - participate in denial of service attacks

Rootkits


ssdpapi .dll WINDOWS\system32 34816
ssdpsrv .dll WINDOWS\system32 71680
ssflwbox.scr WINDOWS\system32 393216
ssmarque.scr WINDOWS\system32 20992
ssmypics.scr WINDOWS\system32 47104
ssmyst .scr WINDOWS\system32 18944
sspipes .scr WINDOWS\system32 610304
ssspl30.ocx WINDOWS\system32 177608
ssstars .scr WINDOWS\system32 14336
sstext3d.scr WINDOWS\system32 679936
Status .MPF WINDOWS\system32 63296
stclient.dll WINDOWS\system32 59392
stdole32.tlb WINDOWS\system32 7168
sti .dll WINDOWS\system32 68096
sti_ci .dll WINDOWS\system32 136704
stimon .exe WINDOWS\system32 14848
stobject.dll WINDOWS\system32 121856
storage .dll WINDOWS\system32 4208
storprop.dll WINDOWS\system32 74752
streamci.dll WINDOWS\system32 8192
strmdll .dll WINDOWS\system32
AskBobRankin.com

Rootkits

- Tools used by attackers after compromising a system
  - hide presence of attacker
  - allow for return of attacker at later date
  - gather information about environment
  - attack scripts for further compromises
- Traditionally trojaned set of user-space applications
  - system logging (syslogd)
  - system monitoring (ps, top)
  - user authentication (login, sshd)

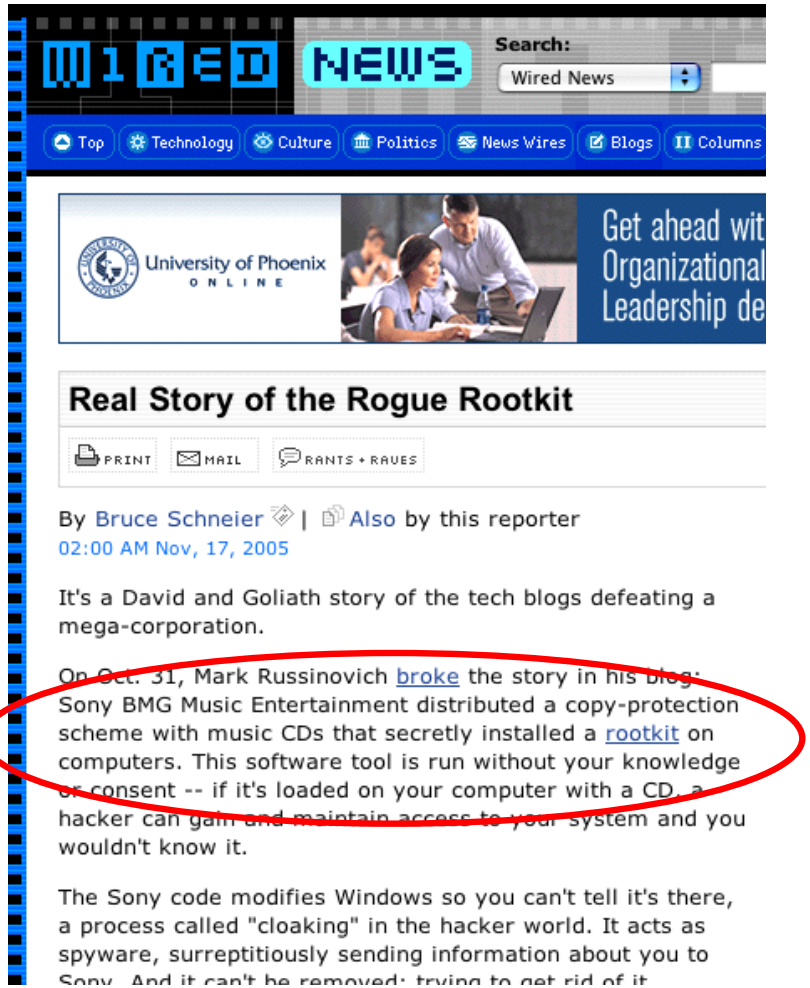
Kernel Rootkits

- Kernel-level rootkits
  - kernel controls view of system for user-space applications
  - malicious kernel code can intercept attempts by user-space detector to find rootkits
- Modifies kernel data structures
  - process listing
  - module listing
- Intercepts requests from user-space applications
  - system call boundary
  - VFS fileops struct

Linux Kernel Rootkits

- Linux kernel exports well-defined interface to modules
- Examples of legitimate operations
  - registering device with kernel
  - accesses to devices mapped into kernel memory
  - overwriting exported function pointers for event callbacks
- Kernel rootkits violate these interfaces
- Examples of illegal operations
  - replacing system call table entries (knark)
  - replacing VFS fileops (adore-ng)

Windows Kernel Rootkits



WIRED NEWS

Search: Wired News

Top | Technology | Culture | Politics | News Wires | Blogs | Columns

Real Story of the Rogue Rootkit

PRINT MAIL RANTS + RAVES

By Bruce Schneier | Also by this reporter
02:00 AM Nov, 17, 2005

It's a David and Goliath story of the tech blogs defeating a mega-corporation.

On Oct. 31, Mark Russinovich broke the story in his blog: Sony BMG Music Entertainment distributed a copy-protection scheme with music CDs that secretly installed a rootkit on computers. This software tool is run without your knowledge or consent -- if it's loaded on your computer with a CD, a hacker can gain and maintain access to your system and you wouldn't know it.

The Sony code modifies Windows so you can't tell it's there, a process called "cloaking" in the hacker world. It acts as spyware, surreptitiously sending information about you to Sony. And it can't be removed; trying to get rid of it

Windows Kernel Rootkits

- Sony rootkit filters out any files/directories, processes and registry keys that contain `$sys$`
- System call dispatcher
  - uses system service dispatch table (SSDT)
  - Windows NT kernel equivalent to system call table
  - entries can be manipulated to re-route call to custom function

`ZwCreateFile`
  - used to create or open file

`ZwQueryDirectoryFile`
  - used to list directory contents (i.e. list subdirectories and files)

`ZwQuerySystemInformation`
  - used to get the list of running processes (among other things)

`ZwEnumerateKey`
  - used to list the registry keys below a given key

Spyware

Spyware

- Any software that monitors and collects information about a user in a covert and unsolicited manner
- Goal of spyware
  - collect sensitive user information and surfing habits
- Task of spyware
  - component must monitor user behavior
  - component must leak information to environment (OS, network)
- Often implemented as browser extensions
  - Internet Explorer Browser Helper Object (BHO)
  - COM object that can hook into Microsoft's Internet Explorer
  - monitor/modify events

Spyware

- Interaction
  - between browser and spyware component
    - COM function invocations (exported by Internet Explorer)
  - between spyware component and operating system
    - Windows API calls

- In addition, it typically has a real company behind it that is making money from the information gathered
  - Adware is any software that injects unsolicited advertisements into a user's workspace
  - Scumware is a specific type of adware that hides other advertisements with those from its own controlling source

Spyware

Typical routes of infection:

1. spyware is bundled with legitimate software package
   - end-user license agreement (EULA) even informs about this fact
   - EULA is very long (often hundreds of pages), user accepts
   - classic examples are shareware programs
     - P2P file-sharing clients (e.g., Kazaa)

2. “drive-by” downloads
   - exploit browser bug, in particular, vulnerabilities of Internet Explorer
   - WMF (Windows meta file) exploit, around Christmas 2005
   - arbitrary code execution via mismatched DOM objects (December 2005)
   - insufficient ActiveX security settings

3. fake dialogs
   - display “Would you like to optimize your Internet” and perform installation when user agrees

Browser Helper Objects (BHOs)

- A BHO is in essence…
  - … a simple Component Object Model (*COM*) object that implements the *IObjectWithSite* interface.
  - IE will load all registered BHOs (that are COM servers) when it starts. It does this by looking at the Class Identifiers (CLSIDs) under
    - \HKLM\SOFTWARE\Windows\CurrentVersion\Explorer\Browser Helper Objects
  - The *IObjectWithSite* interface has a function called *SetSite()*
    - When IE is started, it instantiates the BHO and calls SetSite with a pointer to itself.
    - BHO has access to functions and pointers in IE (e.g., open a new window, etc.)

Useful Spyware Tools

- HijackThis (www.hijackthis.de)
  - Low-level tool, very useful in doing research as well as removal
- Spybot, Adware: Freeware tools
  - Signature based so they do not catch all spyware

Malware and Vulnerable Software

- Malicious software (Malware) and benign software that can be exploited to perform malicious actions (Badware) are two facets of the same problem

  $\longrightarrow$ execution of unwanted code

- Malware
  - viruses, worms, Trojan horses, rootkits, and spyware are evolving to become resilient to eradication and to evade detection
- Badware
  - services and applications (especially web-based) are vulnerable to a wide range of attacks, some of which novel

Rogue Security Software

- A form of Internet fraud using computer malware (malicious software)
  - deceives or misleads users into paying money for fake or simulated removal of malware or claims to get rid of malware, but instead introduces malware to the computer
- Most have
  - Trojan horse component
  - Toolbar or BHO
- Once installed, additional services might be sold by
  - Alerting on fake (simulated) detection of malware
  - Animations of systems crash, or reboots
  - Altering settings, and then alerting user

List of Rogue Software…

- Extensive!

Participate in the world's largest photo competition and help improve Wikipedia!

List of rogue security software

From Wikipedia, the free encyclopedia

This article contains embedded lists that **may be poorly defined, unverified or indiscriminate**. Please help to clean it up to meet Wikipedia's quality standards. *(December 2010)*

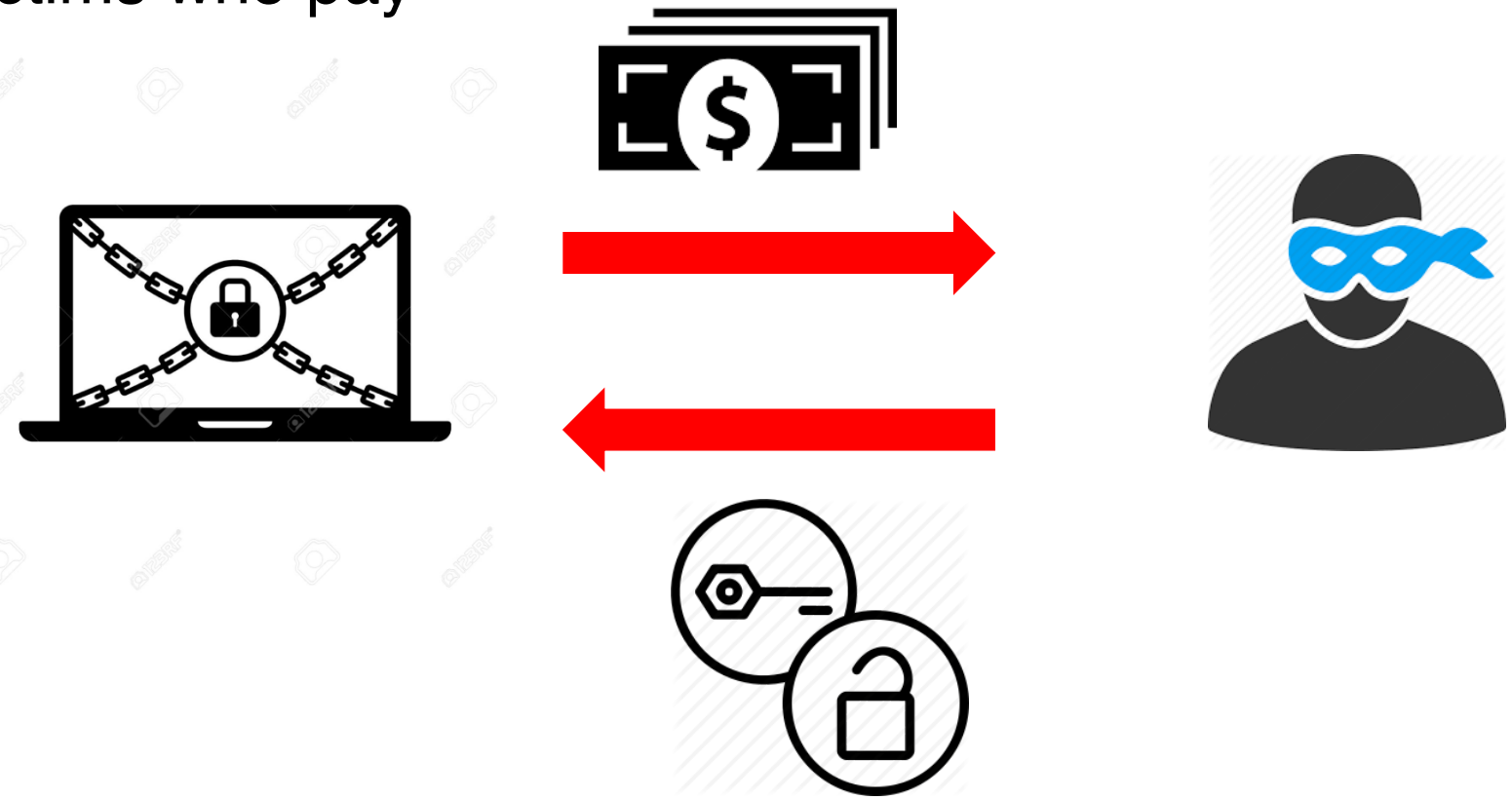
The following is a partial list of rogue security software, most of which can be grouped into *families*. These are functionally identical versions of the same program repackaged as successive new products by the same vendor.

- Advanced Cleaner[3]
- AV Security 2012
- AKM Antivirus 2010 Pro[4]
- AlfaCleaner[5]
- Alpha AntiVirus[6]
- ANG Antivirus (knock-off of AVG Anti-virus)[7]
- Antimalware Doctor[8]
- AntiMalware[9]
- AntiMalware GO[10]
- AntiMalware Go[11]
- AntiSpyCheck 2.1[12]
- AntiSpyStorm[13]
- AntiSpyware 2008[14]
- AntiSpyware 2009[15]
- Antispyware 2010
- AntiSpyware 2011
- AntiSpyware Bot from 2Squared Software
- AntiSpywareExpert[16]
- AntiSpywareMaster[17]
- AntiSpyware Shield[18]
- AntiSpyware Soft[19]
- AntiSpywareSuite[20]
- AntiVermins[21]
- Antivir Solution Pro[22] (not to be confused with Avira AntiVir)
- Antivira AV[23]
- Antivirii 2011[24]
- Antivirus Action[25]
- Antivirus Monitor[26]
- Antivirus 7 or Antivirus5[27]
- Antivirus 8[28]
- Antivirus 8[29]
- Antivirus 360[30]
- Antivirus 2008[31]
- Antivirus 2009[32]
- Antivirus 2010 (also known as Anti-virus-1)[33],[34]
- AntiVirus Gold or AntivirusGT[35]
- Antivirus IS[36]
- Antivirus Live[37],[38]
- Antivirus Master[39]
- Antivirus .NET[40]
- Antivirus Pro 2009[41]
- Antivirus Pro 2010[42]
- Antivirus Scan[43]
- Antivirus Smart Protection[44]
- Antivirus Soft[45]
- ScanAngryAgainAntivirus
- SecureFighter[154]
- SecurePCCleaner[155]
- SecureVeteran[156]
- Security Master AV[157]
- Security Monitor 2012[158]
- Security Protection[159]
- Security Scan 2009[160]
- Security Scanner[161]
- Security Shield[162]
- Security Solution 2011[163]
- Security Suite Platinum[164]
- Security Tool[165]
- Security Tool[166]
- Security Toolbar 7.1[167]
- Security Essentials 2010 (not to be confuse
- SiteAdware
- SkyVast Anti-Virus 2011
- Smart Anti-Malware Protection[169]
- Smart Antivirus 2009[170]
- Smart Engine[171]
- Smart HDD[172]
- Smart Protection 2012[173]
- Smart security[174]
- Soft Soldier[175]
- Spy Away[176]
- SpyAxe[177]
- SpyBouncer
- SpyCrush[178]
- Spydawn[179]
- SpyEraser[180] (Video demonstration)
- SpyGuarder[181]
- SpyHeal (a.k.a. SpyHeals & VirusHeal)[182]
- Spylocked[183]
- SpyMarshal[184]
- SpyRid[185]
- SpySheriff (a.k.a. PestTrap, BraveSentry, S
- SpySpotter[187]
- Spy Tool
- SpywareBot (Spybot - Search & Destroy kn
- Spyware Cleaner or Spyware Blaster[189]
- SpywareGuard 2008 (not to be confused wit
- spyware NO
- Spyware Protect 2009[192]
- Spyware Protect 2009[193]

Example Dialogs

Ransomware

1. Encrypting user data
2. Requesting the ransom fee
3. Sending the decryption key to victims who pay



Attack Implementation

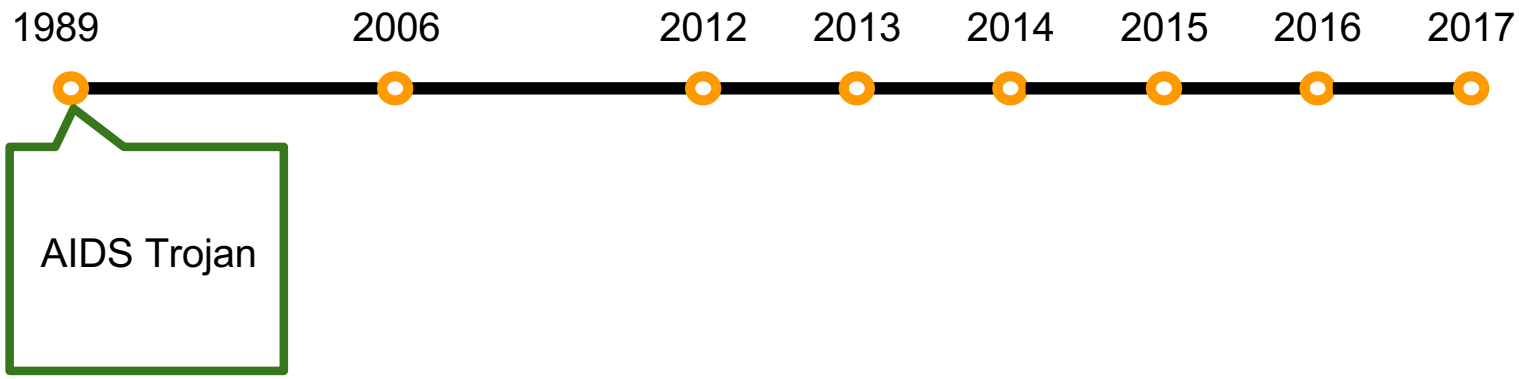
- A successful attack relies on a reliable cryptosystem
  - A cryptosystem is a pair of algorithms that take a key and convert plaintext to ciphertext and back.
  - Malware authors user cryptosystems to encrypt user data and force the victims to pay
  - Modern ransomware make use of standard cryptosystem that the OS provides (i.e., Microsoft CryptoAPIs)

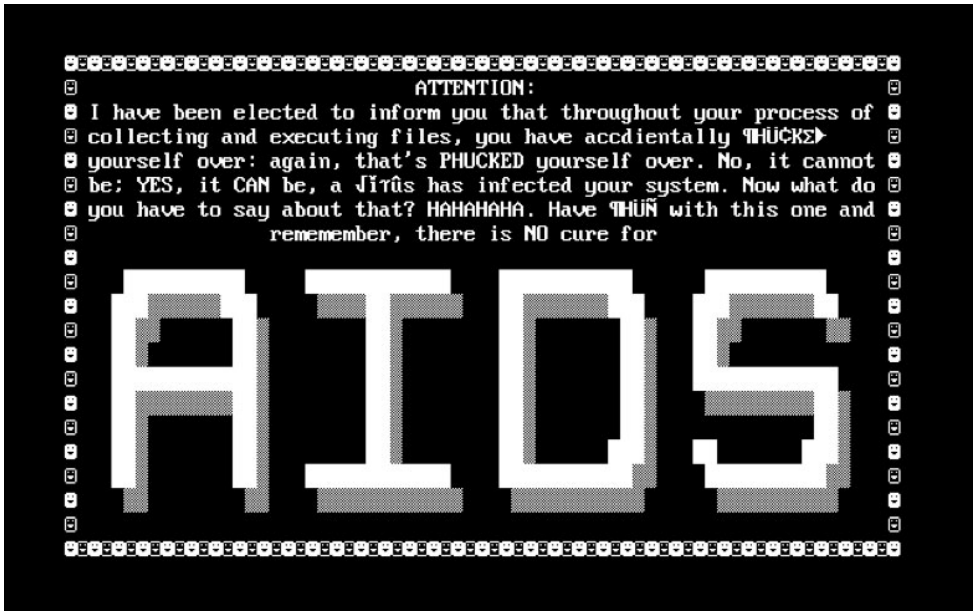
- A successful attack also requires reliable methods to request payments:
  - More and more ransomware attacks use Bitcoin transactions,why?
    - Hard to trace
    - The laundry services in Bitcoin ecosystem make the traceability even harder

Ransomware Origin

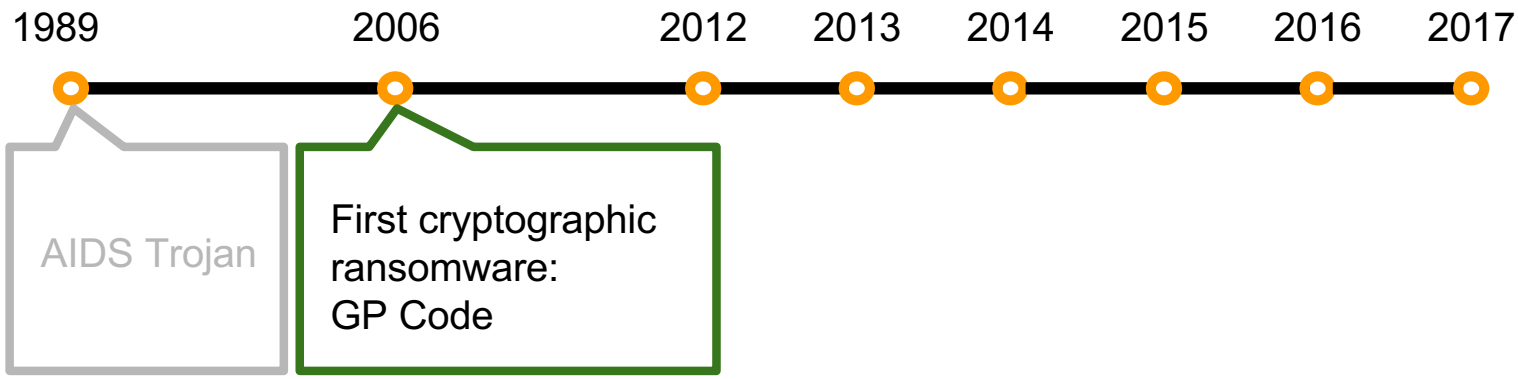
- The first type of ransomware, AIDS Trojan, dates back 26 years ago
  - Written in QuickBasic 3.0
  - The program modifies the AUTOEXEC.BAT
  - After 90 reboots, the user gets a warning
  - The payment was $189 to obtain a repair tool
- Despite the public being unprepared, AIDS was ultimately unsuccessful
  - Few people used computers
  - The availability encryption technology was somewhat limited at the time

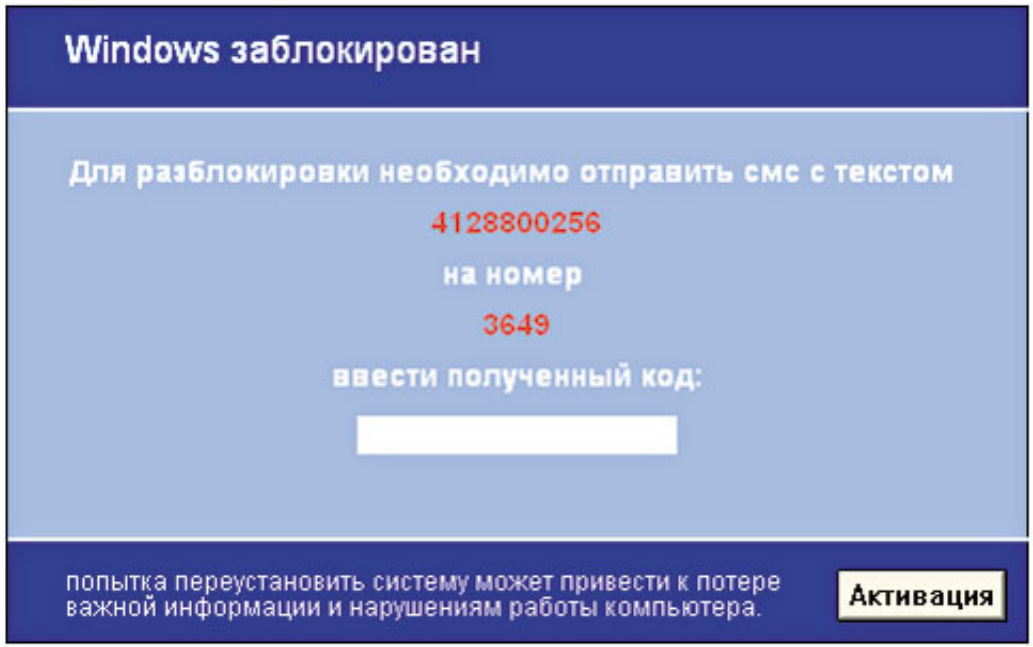
Ransomware History



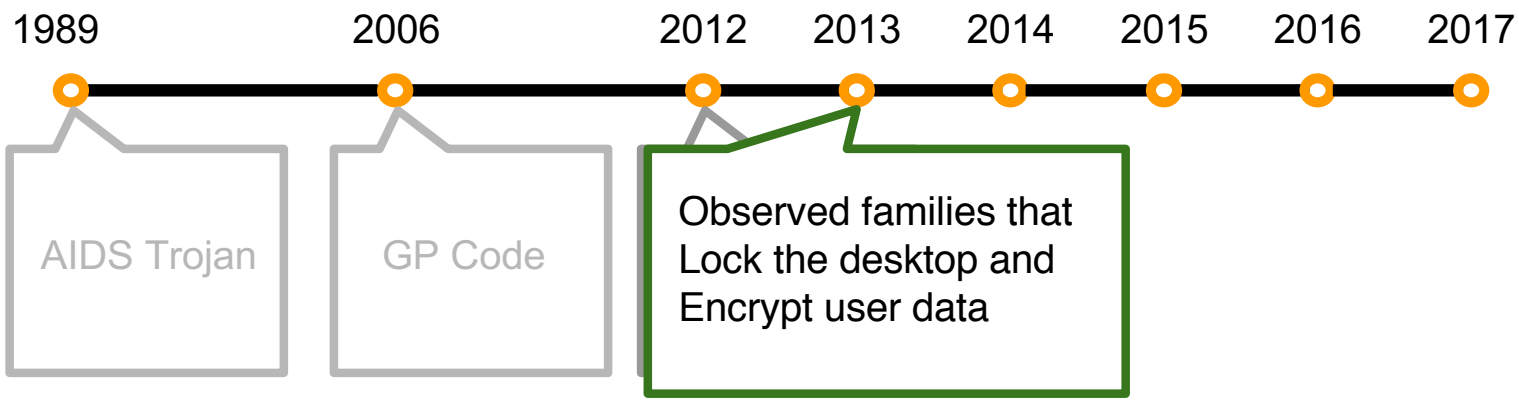


Ransomware History

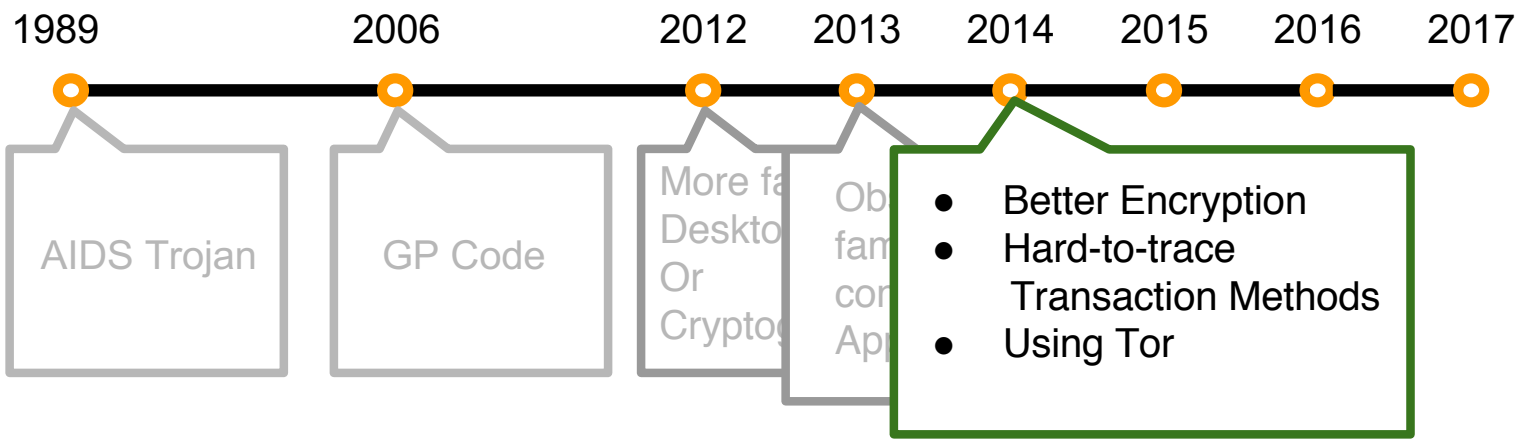




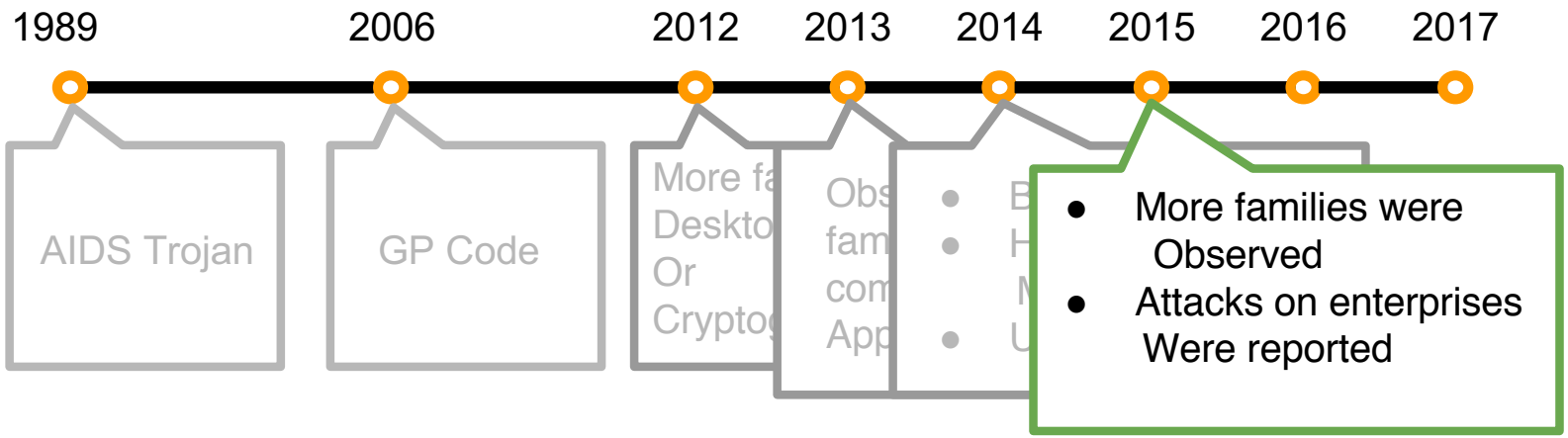
Ransomware History



Ransomware History



Ransomware History



Home ▸ Tewksbury Town Crier ▸ News

Police pay ransom after cyberterror attack on network

Story | Comments (1) | Print | Font Size:

Thomas Murphy, Daniel Sawicki and Lt. Scott Keddie

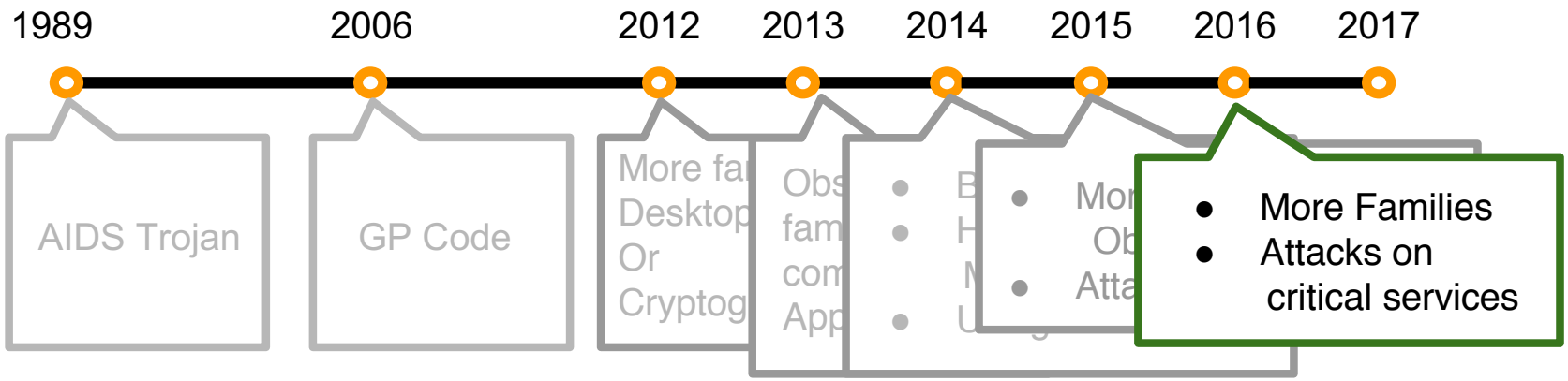
Posted: Saturday, April 4, 2015 10:27 am

By Jayne W. Miller News Editor
Jayne@YourTownCrier.com | 1 comment

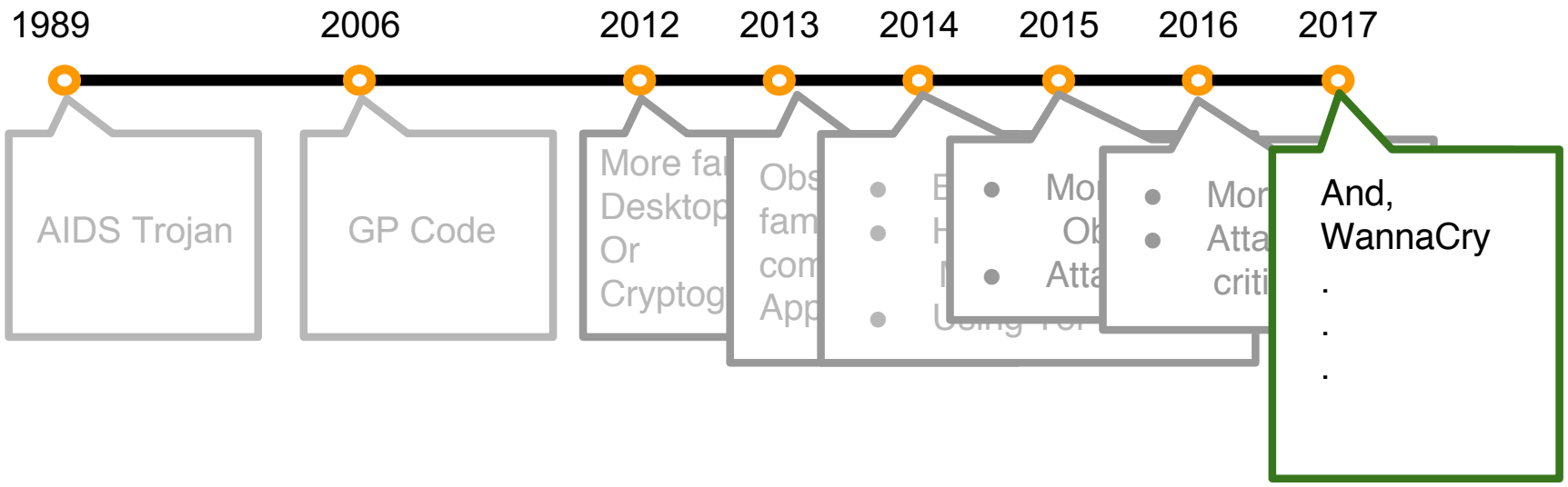
Chief: "Paying ransom was the last resort"

TEWKSBURY – Last December Tewksbury Police confronted a new, and growing, frontier in cyberterrorism when the CryptoLocker ransomware virus infected the department's network, encrypting essential department files until the town paid a $500 bitcoin ransom. In total, police systems were down between four and five days as the department worked with the FBI, Homeland Security, Massachusetts State Police, as well as private firms in an effort to restore their data without paying the ransom.

Ransomware History



Ransomware History



JUN 22, 2017 @ 05:00 AM 7,241

12 Stocks to Buy Now

Cyber Attack At Honda Stops Production After WannaCry Worm Strikes

Peter Lyon, CONTRIBUTOR

I write about automobiles and games. FULL BIO

Opinions expressed by Forbes Contributors are their own.

TECH | CYBERSECURITY

UK hospitals hit with massive ransomware attack

Sixteen hospitals shut down as a result of the attack

by Russell Brandom | @russellbrandom | May 12, 2017, 11:36am EDT

SHARE TWEET LINKEDIN

Ransomware Attacks

So, why is ransomware interesting from malware research perspective?

- Less stealthy (e.g., you're told that you are infected!)
- Usually has a distinctive behavior, why?