Computing in the presence of an adversary

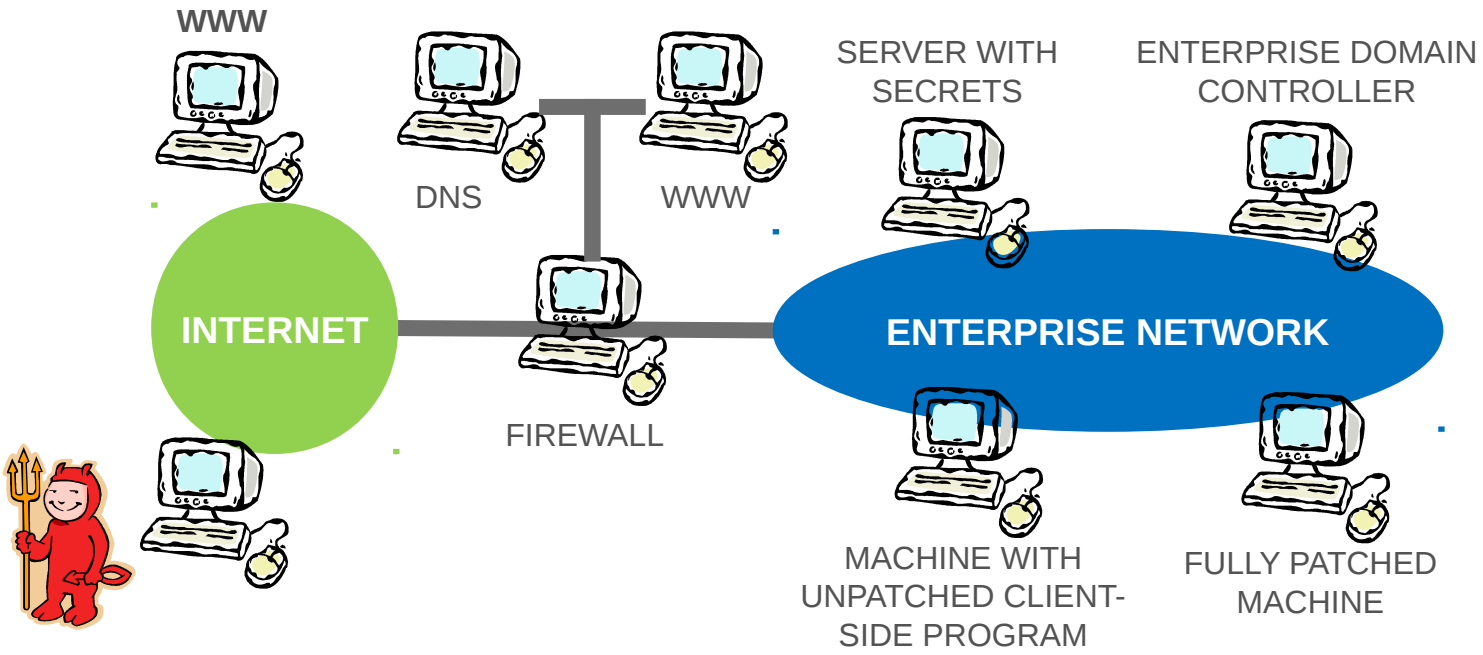
Lecture plan

- **Intro and attacker modus**
- Software and web app security
- System security
- Cryptography
- Network security
- Reactive security
- Outro

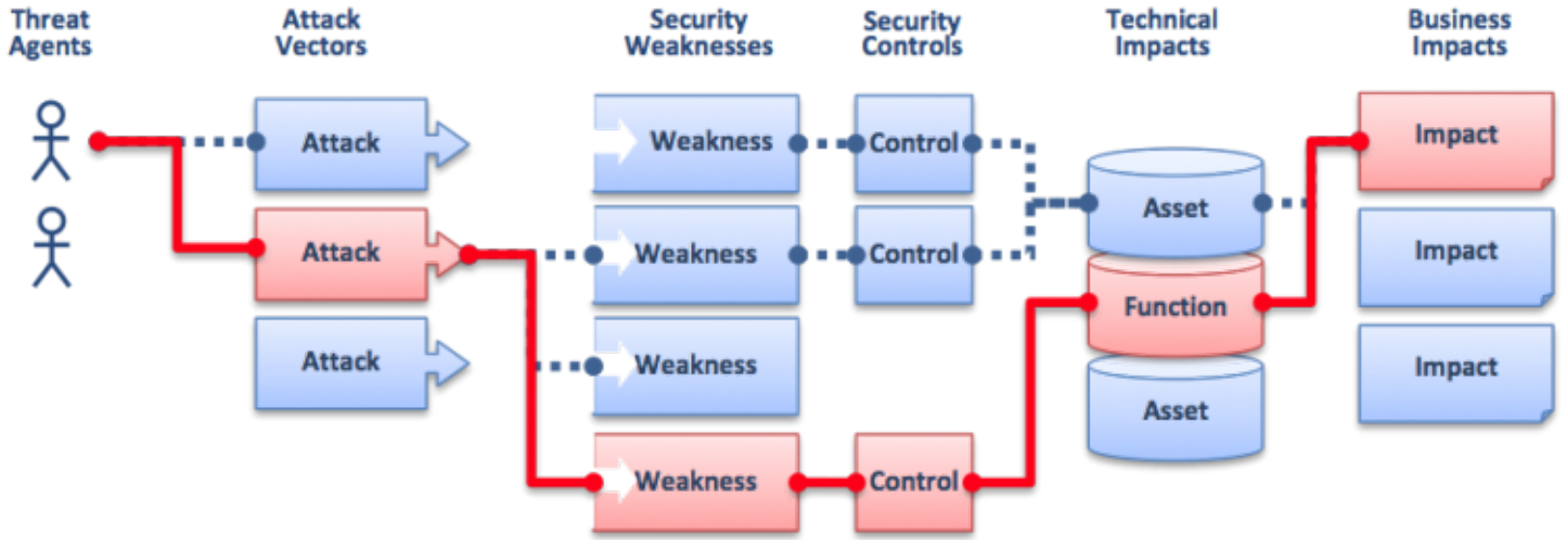
Today's agenda

- Attacker MO
- Threat actors

Situation


WWW
DNS
WWW
SERVER WITH SECRETS
ENTERPRISE DOMAIN CONTROLLER
INTERNET
FIREWALL
ENTERPRISE NETWORK
MACHINE WITH UNPATCHED CLIENT-SIDE PROGRAM
FULLY PATCHED MACHINE

Chain of events



Exploit catagories

- Server-side
  - Exploits vulnerabilities in listening services
- Client-side
  - Exploits vulnerabilities in client applications such as PDF readers, browsers
- Local privilege escalation
  - Exploits that jump from limited accounts to more powerful ones

Vulnerabilities, exploits and malware

- Vulnerability
  - A bug in a piece of software
- Exploit
  - Code that takes advantage of a vulnerability
- Zero-day
  - Previously unknown vulnerability and/or exploit
- Malware
  - Malicious software to maintain unauthorised access, gather private information, disrupt operations, delete data, etc.

Attack vector

- A means to deliver the exploit / malware

- Top vectors include
  - Email
  - Drive-by downloads
  - Vulnerable Internet-facing service
  - Web application attacks

Attack surface

- Not just the browser, but the browser and all the plug-ins and extensions, and the OS libraries the browser calls – this is the **attack surface**

It starts with *Intent*

Anticipating Intent

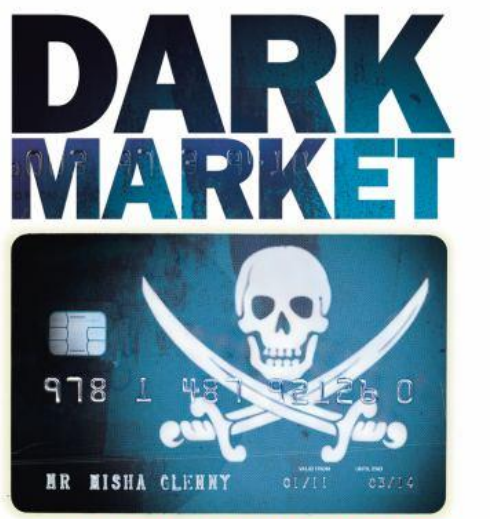
- “Our competitors got hacked”
- “We're negotiating a big contract”
- “We're participating in this big conference”
- “We're getting this particular press coverage”

- “Everybody else is getting hacked”

Flat out Intent

'Hacktivists' threaten to destroy Facebook on November 5 over privacy policy

Sniffing out Intent



KEVIN POULSEN 10.13.08 1:20 PM

CYBERCRIME SUPERSITE 'DARKMARKET' WAS FBI STING, DOCUMENTS CONFIRM

Spying on Intent

The NSA knew North Korea hacked Sony because it hacked North Korea first

by Steve Dent | @stevetdent | January 19th 2015 at 8:38 am

159

Target selected. Start: *Recon*

Recon

- Passive
  - Gather information from public sources to learn about the target
- Active
  - Interact with victim systems, perhaps scanning them

Job adds

Information Security Manager

Job Number: 73390712

Company Name: Regions Financial

Location: Hoover, AL US

Career Focus: Accounting & Finance Updated: 3/23/2013

Directs a team responsible for information systems security to ensure the protection of information processed, stored and transmitted. Determines user requirements, plans projects,

Types of systems in use:
Snort Network Intrusion Detection System (with RedHat Linux OS)
IBM Tivoli Security Operations Manager (plan to migrate to ArcSight in 2013) -- used for Security Information Event Management
HP TippingPoint Intrusion Prevention System (IPS)
Aruba Wireless Intrusion Detection System
Cisco Security Agent and Bit9 for workstation, laptop, ATM, and server anti-malware -- migrating off Cisco to Bit9 by EOY 2013
Syslog server with RedHat Linux OS
IP Recorders
UNIX security for Solaris, AIX, and RedHat; (LDAP used for security)

“Google hacking”

Google hacking

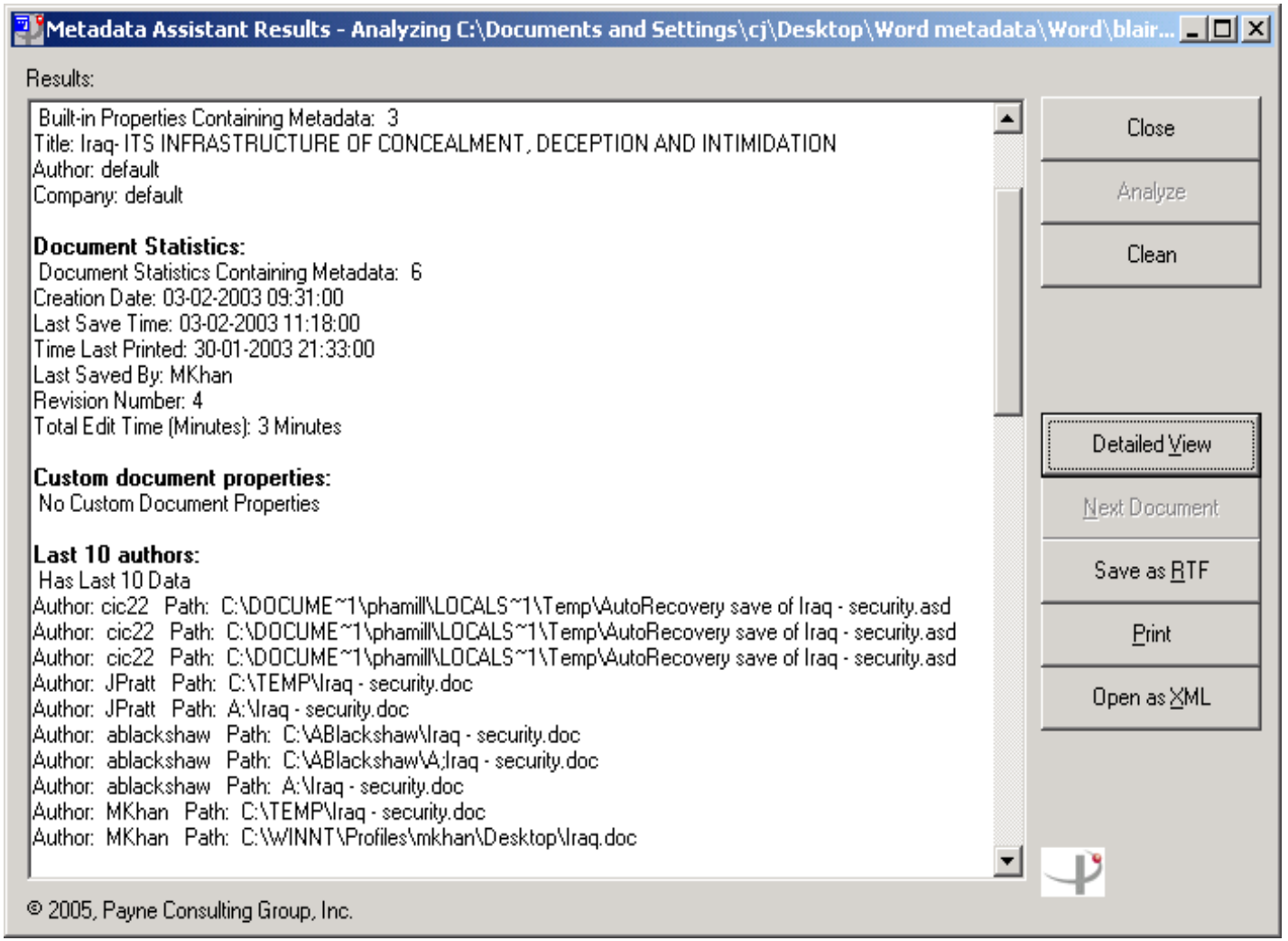
From Wikipedia, the free encyclopedia

Not to be confused with Google Hacks.

Google hacking, also named **Google dorking**,[1][2] is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use.

Crawl entire web site

Document metadata



Whois information

- When a domain name is registered, the registrar registers information like
  - People associated with the domain
  - Domain Name System (DNS) servers
- Whois is both a TCP service, tool and type of database

Domain Name Service (DNS)

- Phone book of the Internet
- Naming system and domain name to IP lookup
- Records for differnet types of systems
  - A: address record
  - MX: mail server record
  - NS: name server record

Let’s try it out...

So we got our targets

Scanning

- Host discovery
- Port scanning
- OS fingerprinting
- Version detection
- Vulnerability scanners

Host discovery - ICMP

- ICMP is a supporting protocol to send error messages and operational information
  - Type 8, code 0 = echo request
  - Type 0, code 0 = echo reply

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Header Checksum	
	Source IP address			
	Destination IP address			
ICMP Header (8 bytes)	Type of message	Code	Checksum	
	Header Data			
ICMP Payload (*optional*)	Payload Data			

Host discovery - ICMP

```
#try it out
$ ping dr.dk

#ping localhost and record session
$ ping -c 2 localhost
$ sudo tcpdump -i lo icmp -w ping.pcap

#ping sweep
$ for i in {1..254}; do ping -c 1 -W 1 192.168.184.$i; done
```

Host discovery - ARP

- ARP is used for discovering the link layer address associated with a given IP address

```
[...]
17:17:29.340410 ARP, Request who-has 192.168.184.138 tell
192.168.184.1, length 28
17:17:29.342788 ARP, Request who-has 192.168.184.139 tell
192.168.184.1, length 28
17:17:29.344785 ARP, Request who-has 192.168.184.140 tell
192.168.184.1, length 28
17:17:29.346244 ARP, Reply 192.168.184.140 is-at
00:50:56:e9:42:d2 (oui Unknown), length 28
[...]
```

- Lookup MAC OUI
  - standards-oui.ieee.org/oui/oui.txt

Passive host discovery

- A packet sniffer is a program that intercepts and logs traffic that traverses its hosts network interface controller

Port scanning - TCP

```
$ man nmap
-sS (TCP SYN scan)
-sT (TCP connect scan)
-sF (FIN scan)

$ cat tcp-scan-expections
SYN-ACK = port open
RST-ACK = port closed
No response = filtered?
```

Port scanning - UDP

```
$ man nmap
-sU (UDP scan)

$ cat udp-scan-expections
Reply = port open
No reply = open or filtered
ICMP port unreachable = port closed
ICMP host unreachable = filtered
```

OS fingerprinting

- Many methods
  - IP TTL, ID, ..
  - TCP Window size, Options, ..
  - DHCP requests
  - ICMP requests
  - HTTP packets (generally, User-Agent field)

OS fingerprinting

```
$ firefox nmap.org/book/osdetect-methods.html

$ sudo nmap -sT -O 192.168.184.140

Running: Microsoft Windows 2008|7
OS CPE: cpe:/o:microsoft:windows_server_2008::sp2
cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_8
OS details: Microsoft Windows Server 2008 SP2, Microsoft
Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
```

Version detection

```
# service scan with nmap
$ nmap -sT -sV -p 139,445 192.168.184.148

Starting Nmap 6.40 ( http://nmap.org )
Nmap scan report for 192.168.184.148
Host is up (0.00053s latency).
PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X (workgroup: Uni)
445/tcp open  netbios-ssn Samba smbd 3.X (workgroup: Uni)
```

Vulnerability scanning

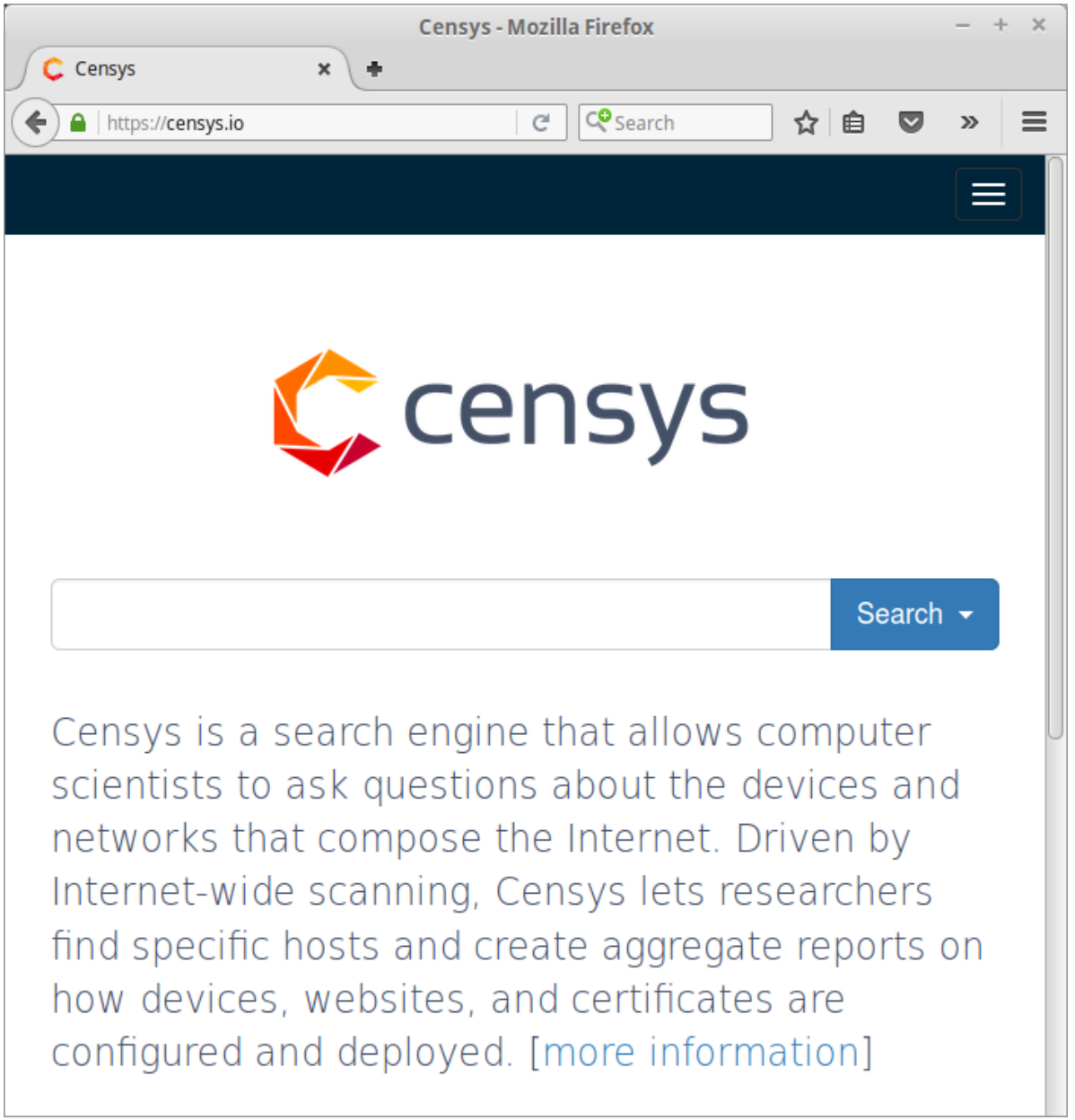
```
# investigate for known issues
$ firefox google.dk/search?q=Samba+smbd+3.X
$ firefox cvedetails.com/vulnerability-list/vendor_id-
102/Samba.html

# automate with built-for-the-purpose applications
$ cat some-vuln-scanners
Nmap nse
Nessus
OpenVAS
...
```

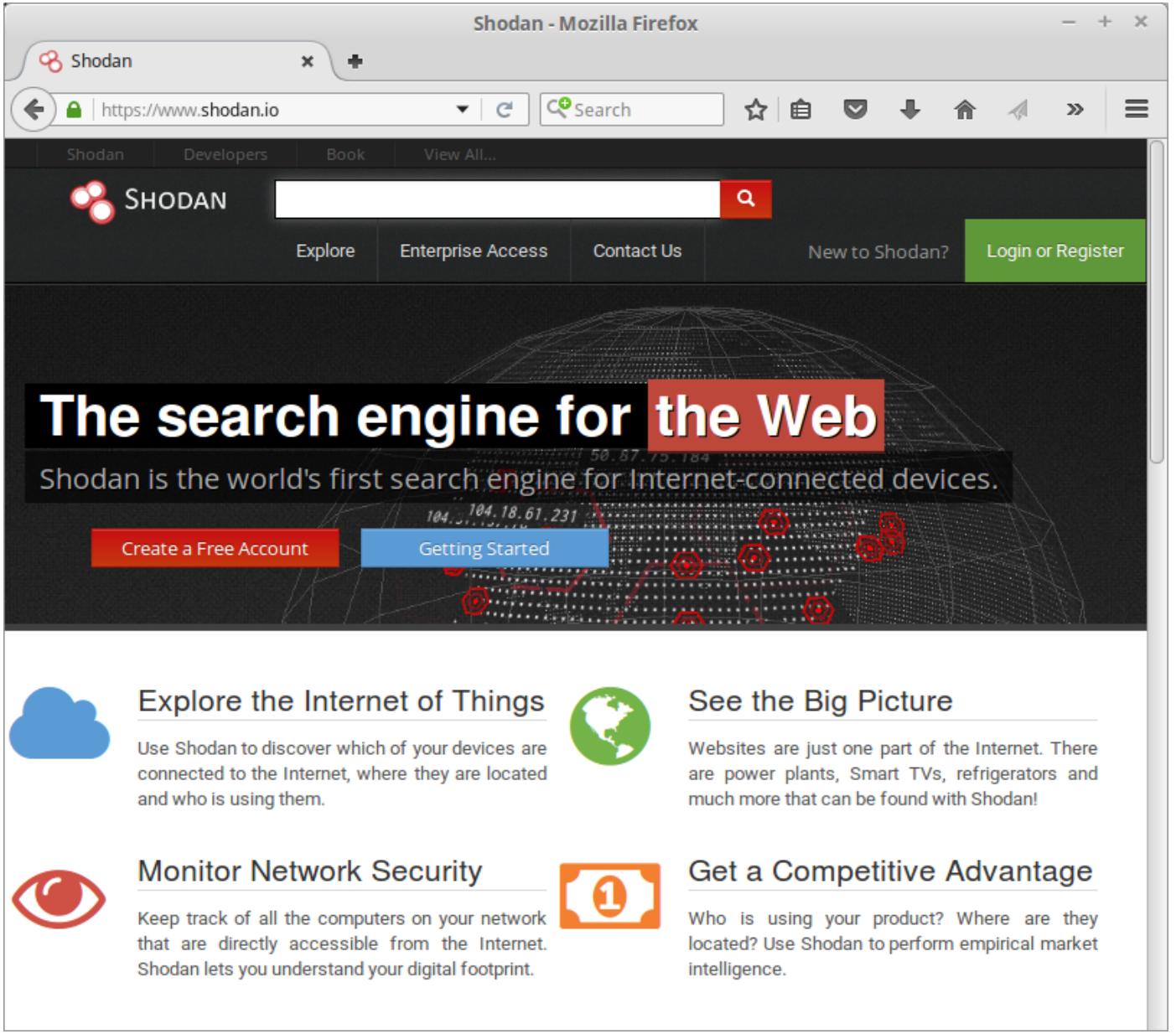
Or DIY

- Find a new vulnerability and exploit it
- ... Next time

Censys.io


Censys - Mozilla Firefox
Censys
https://censys.io
Search
censys
Search
Censys is a search engine that allows computer scientists to ask questions about the devices and networks that compose the Internet. Driven by Internet-wide scanning, Censys lets researchers find specific hosts and create aggregate reports on how devices, websites, and certificates are configured and deployed. [more information]

Shodan.io


Shodan - Mozilla Firefox
Shodan
https://www.shodan.io
Search
Shodan
Developers
Book
View All...
SHODAN
Explore
Enterprise Access
Contact Us
New to Shodan?
Login or Register
The search engine for the Web
Shodan is the world's first search engine for Internet-connected devices.
Create a Free Account
Getting Started
Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.
See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!
Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.
Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Exploit DB

Remote Exploits

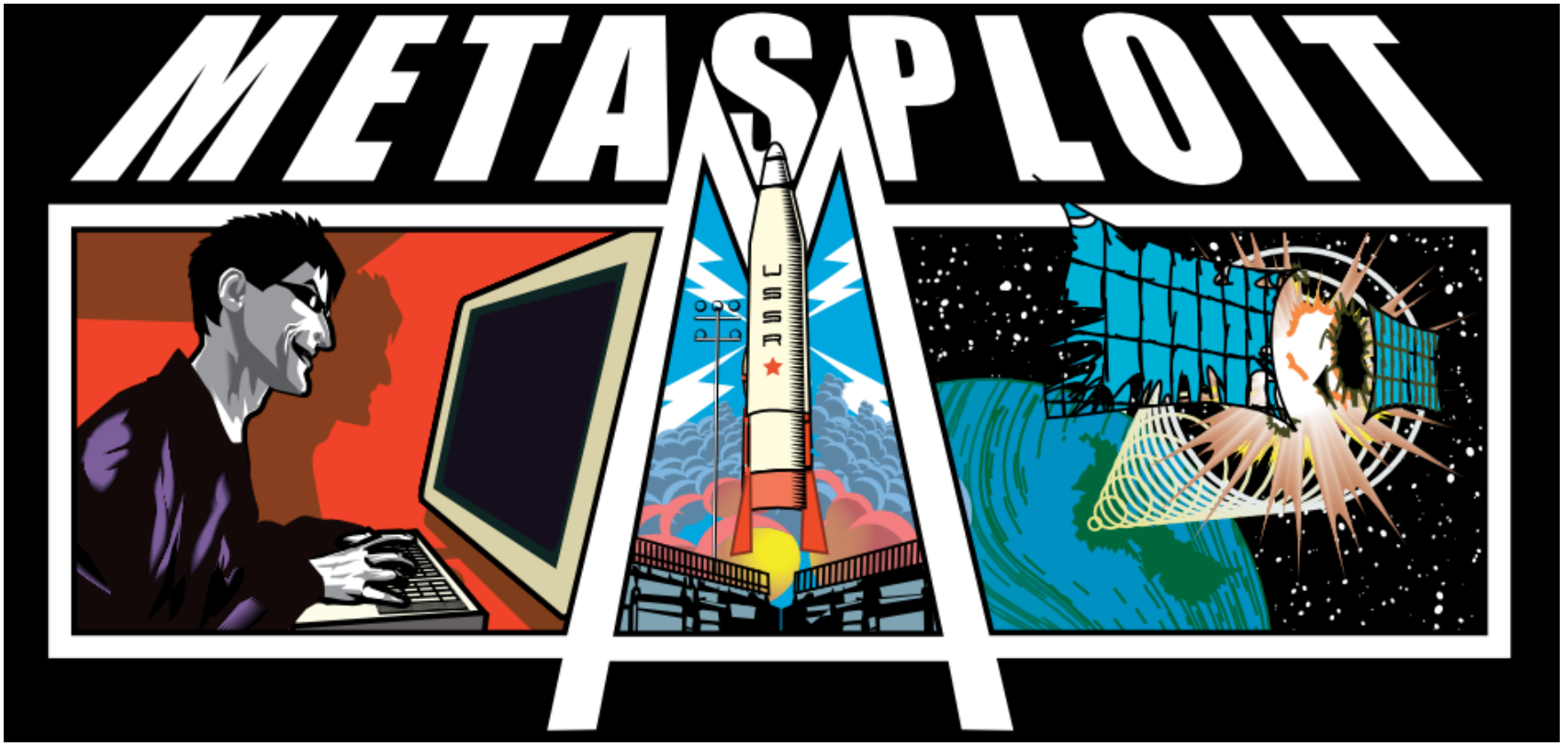
This exploit category includes exploits for remote services or applications, including client side exploits.

Date	D	A	V	Title	Platform	Author
2016-04-26		-		Advantech WebAccess Dashboard Viewer Arbitrary File Upload	windows	metasploit
2016-04-26		-		libgd 2.1.1 - Signedness Heap Overflow	linux	Hans Jerry Ill.
2016-04-25				PCMan FTP Server 2.0.7 - RENAME Command Buffer Overflow (MSF)	win32	Jonathan Smith
2016-04-18		-		Novell ServiceDesk Authenticated File Upload	multiple	metasploit
2016-04-14		-		Internet Explorer 9, 10, 11 - CDOMStringDataList::InitFromString Out-of-Bounds Read (MS15-112)	windows	Ashfaq Ansari
2016-04-13		-		Dell KACE K1000 File Upload	unix	metasploit
2016-04-05				Easy File Sharing HTTP Server 7.2 SEH Overflow	windows	metasploit

Web Application Exploits

Metasploit

- Exploitation made easy

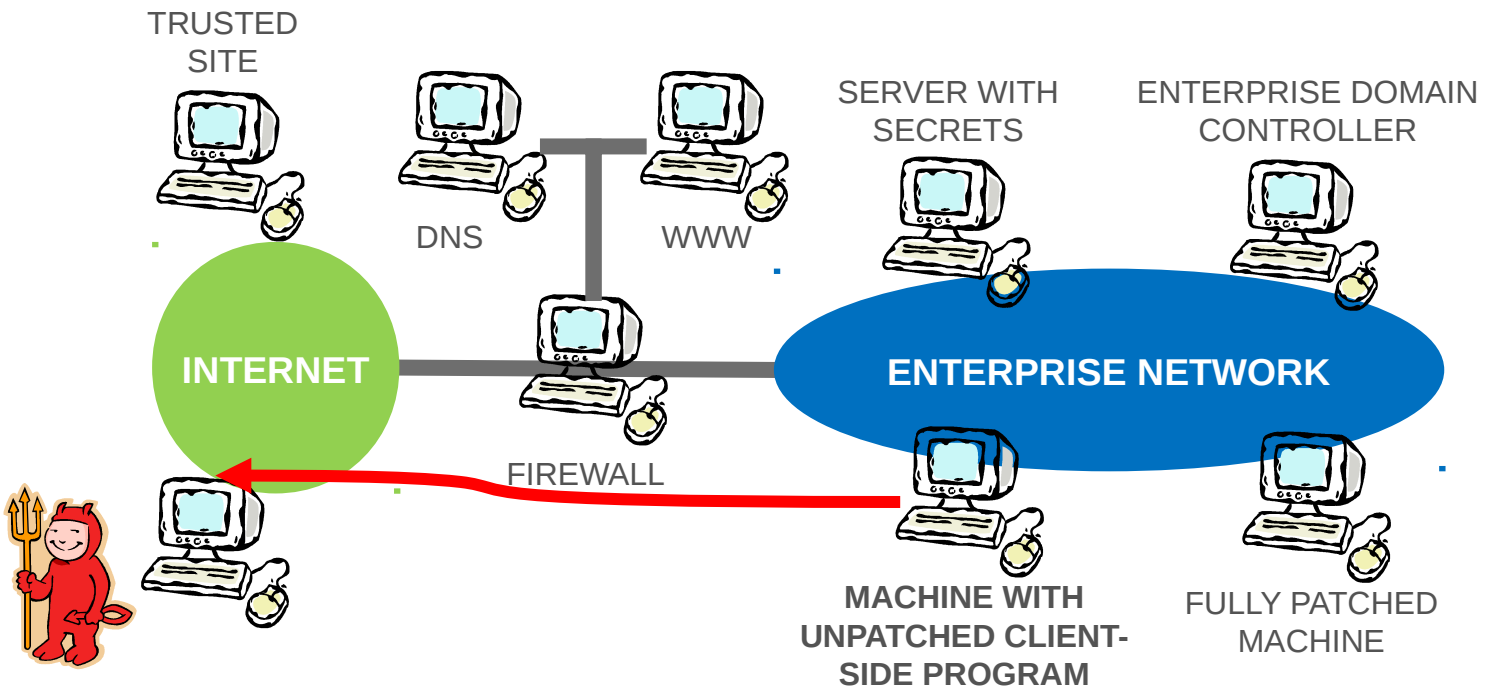


Post-exploitation

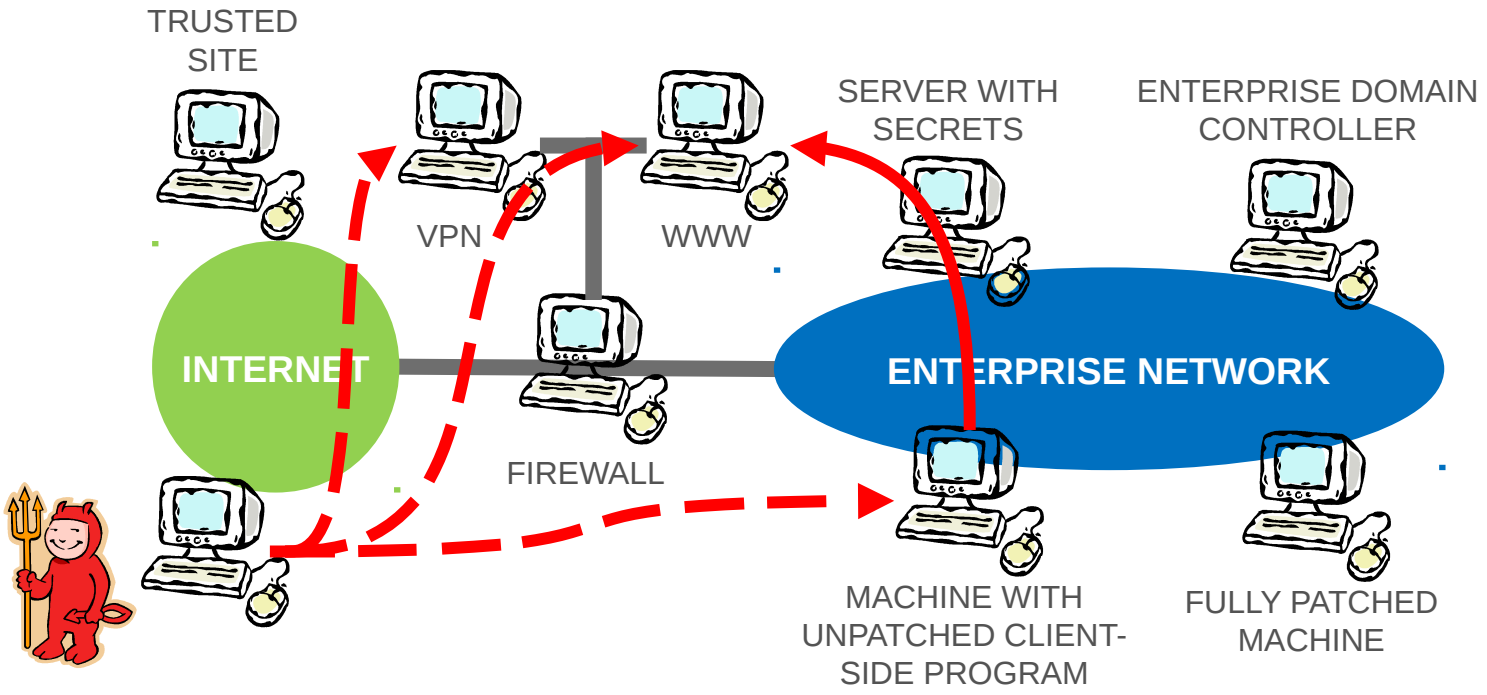
Post-exploitation

- Install
- Command and control
- Action on Objectives

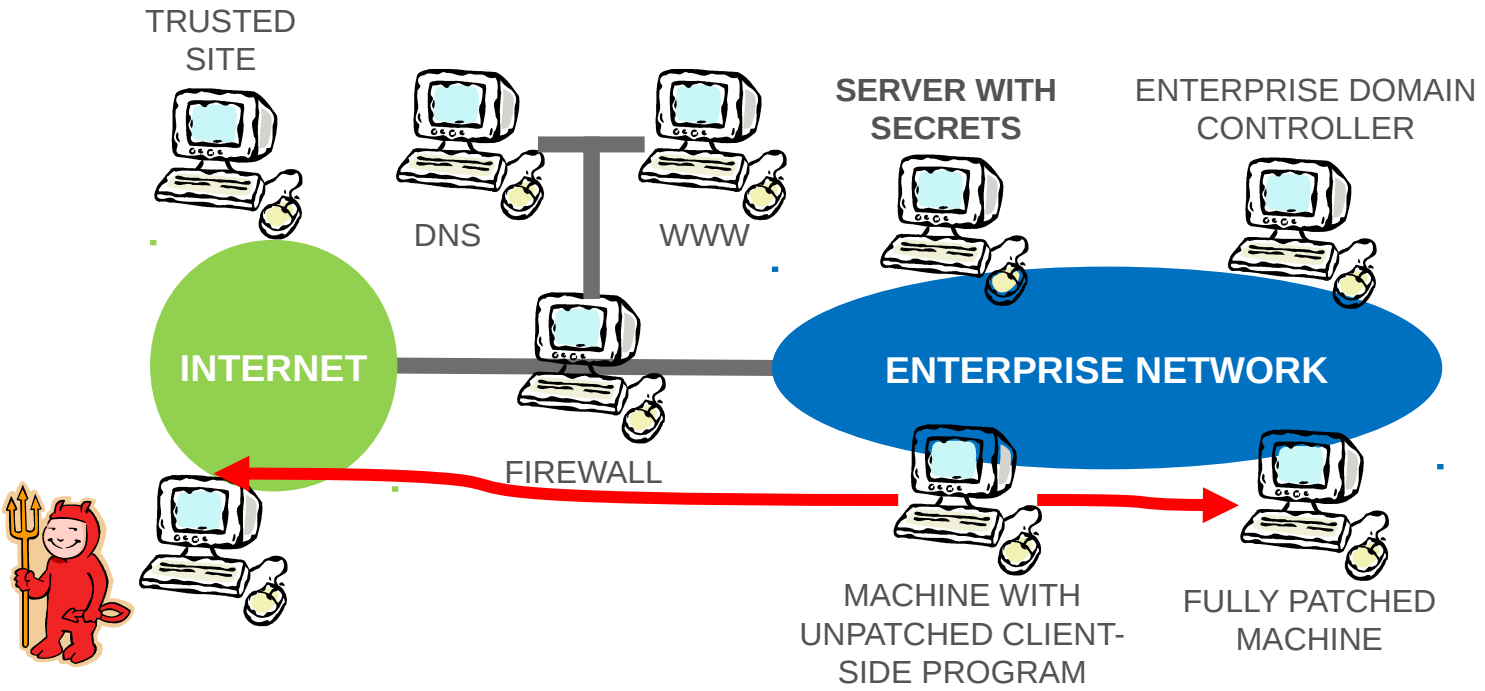
Install and beacon



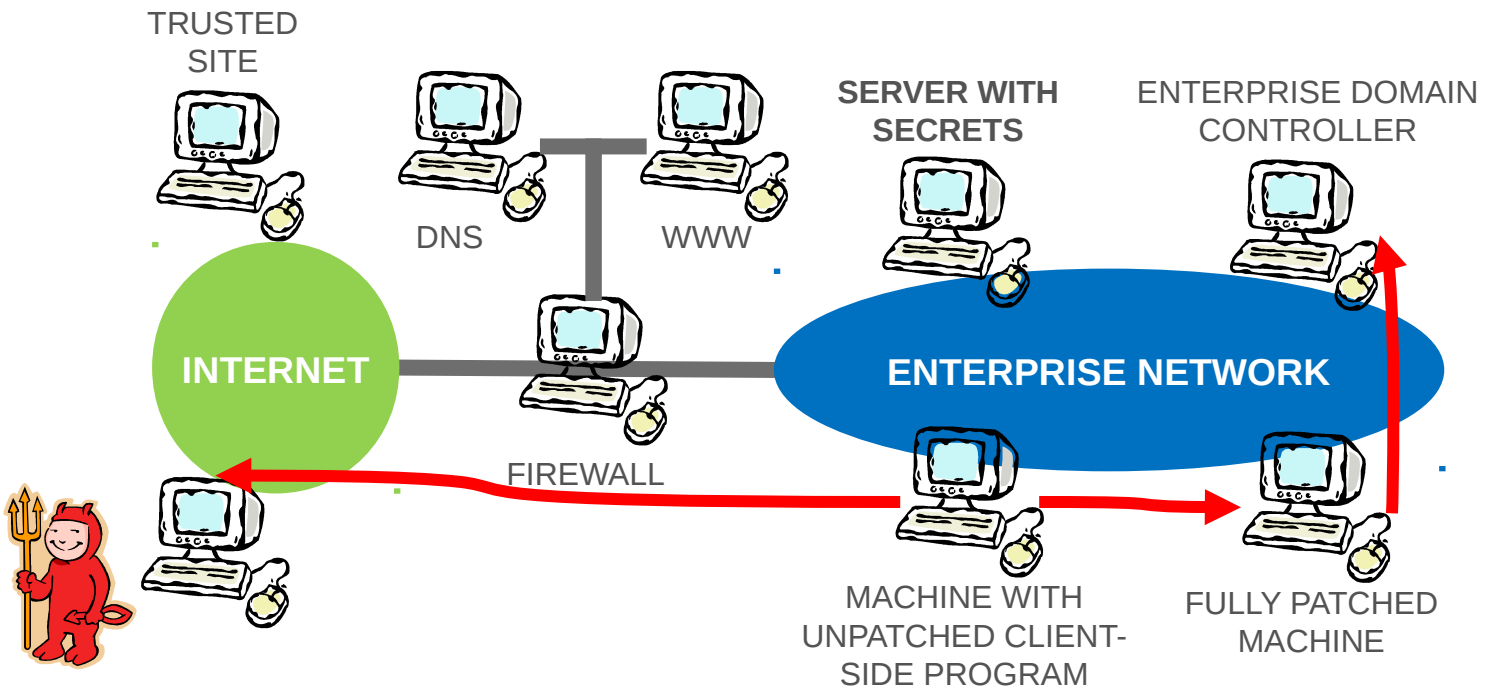
Keeping access



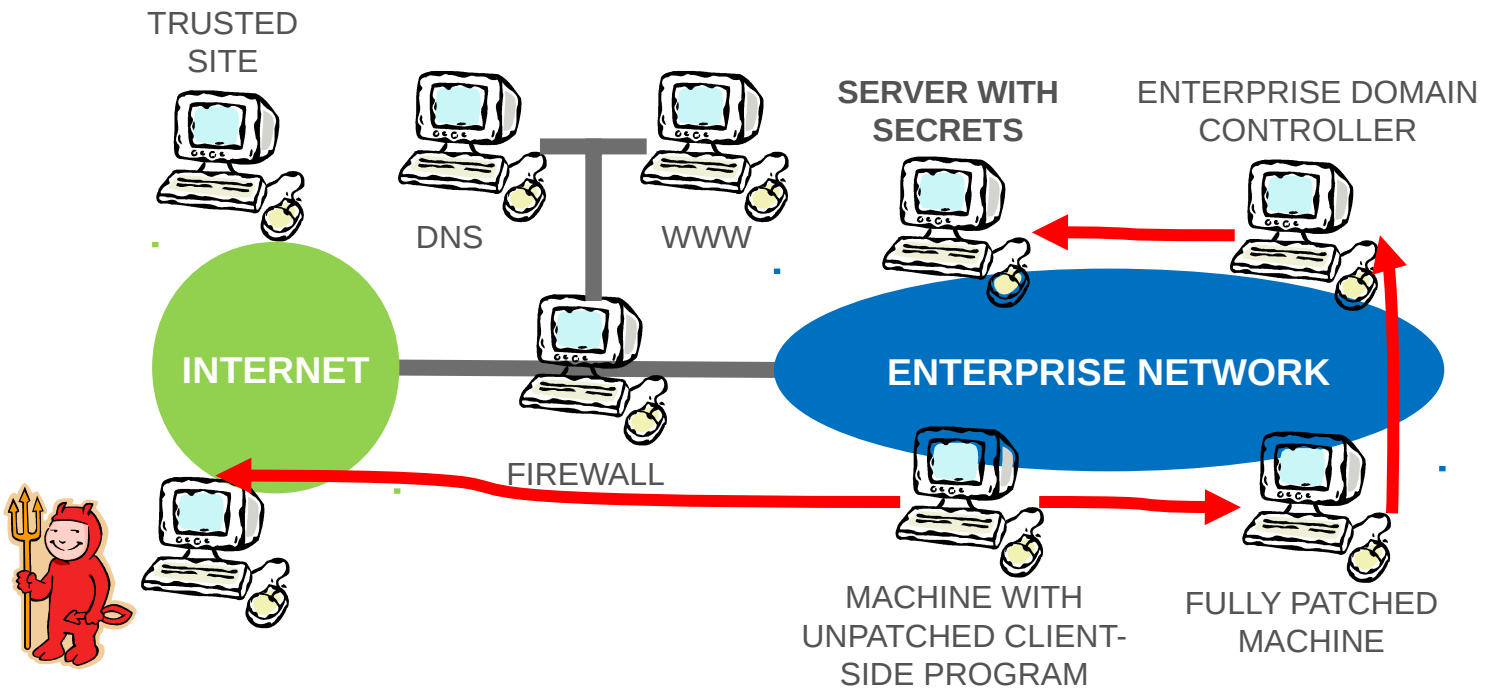
Lateral movement



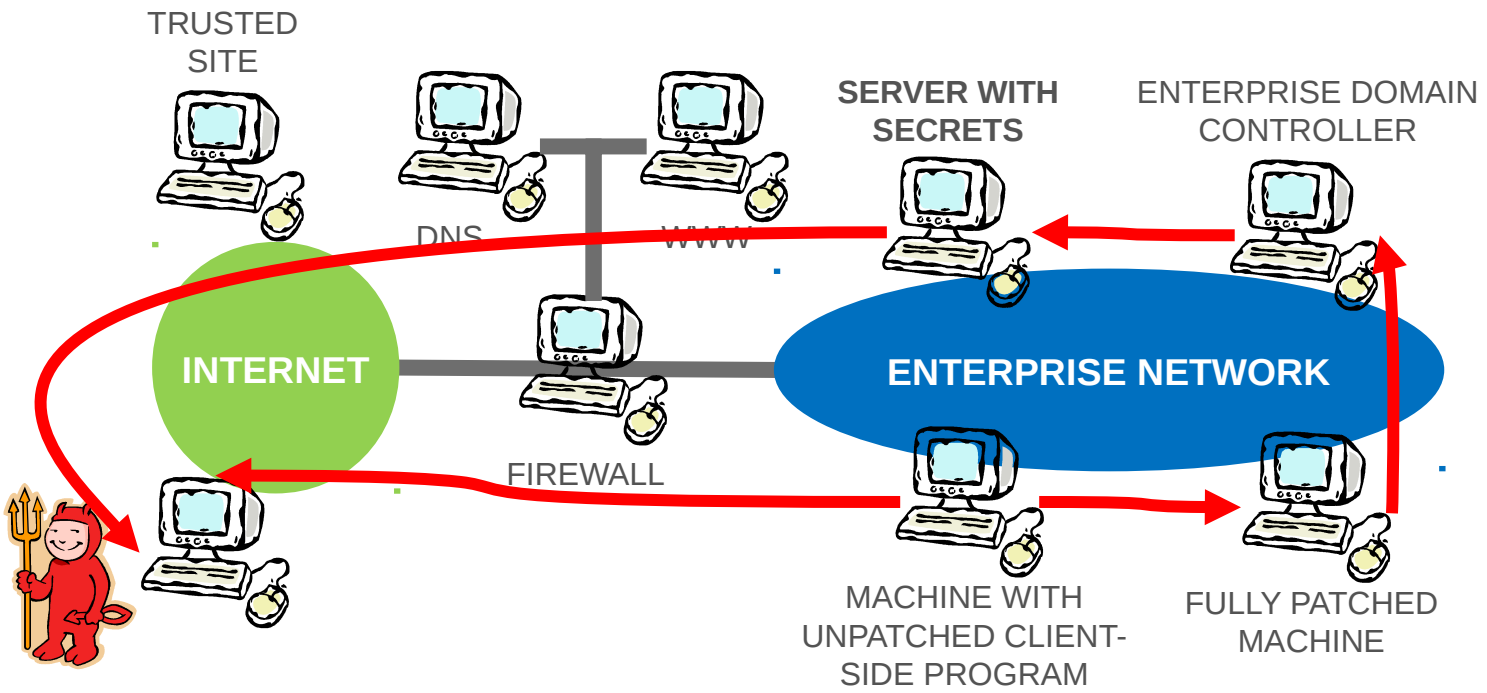
Lateral movement



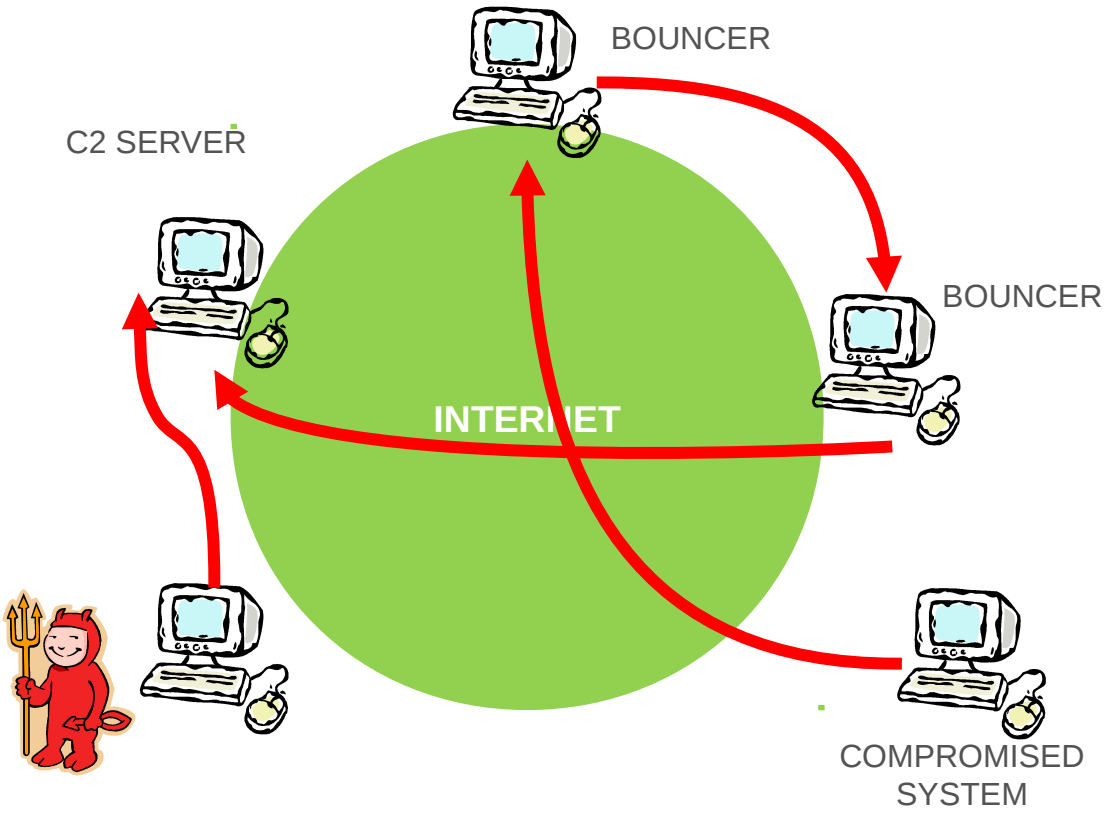
Lateral movement



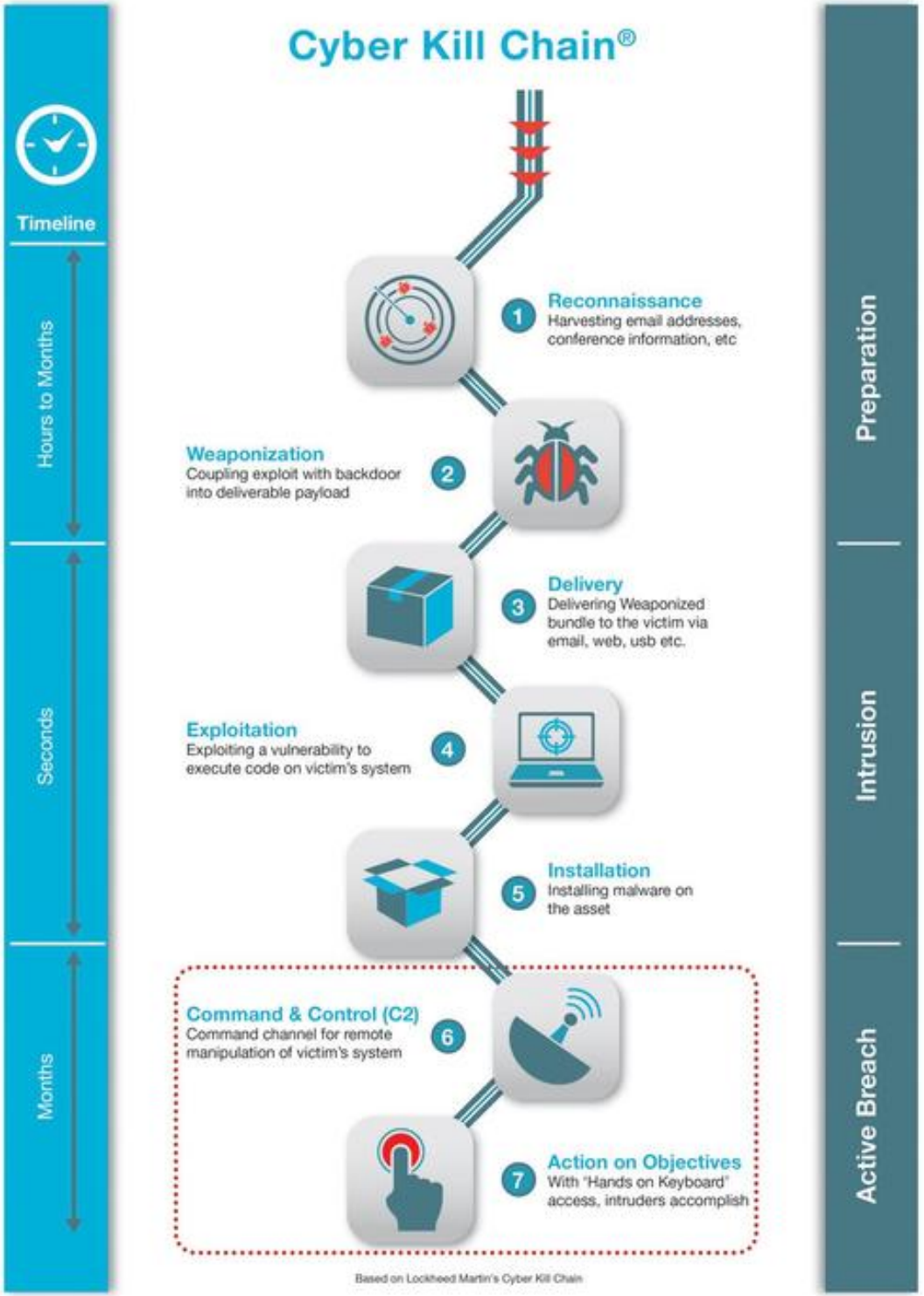
Complete the mission



Layers of



Cyber Kill Chain®

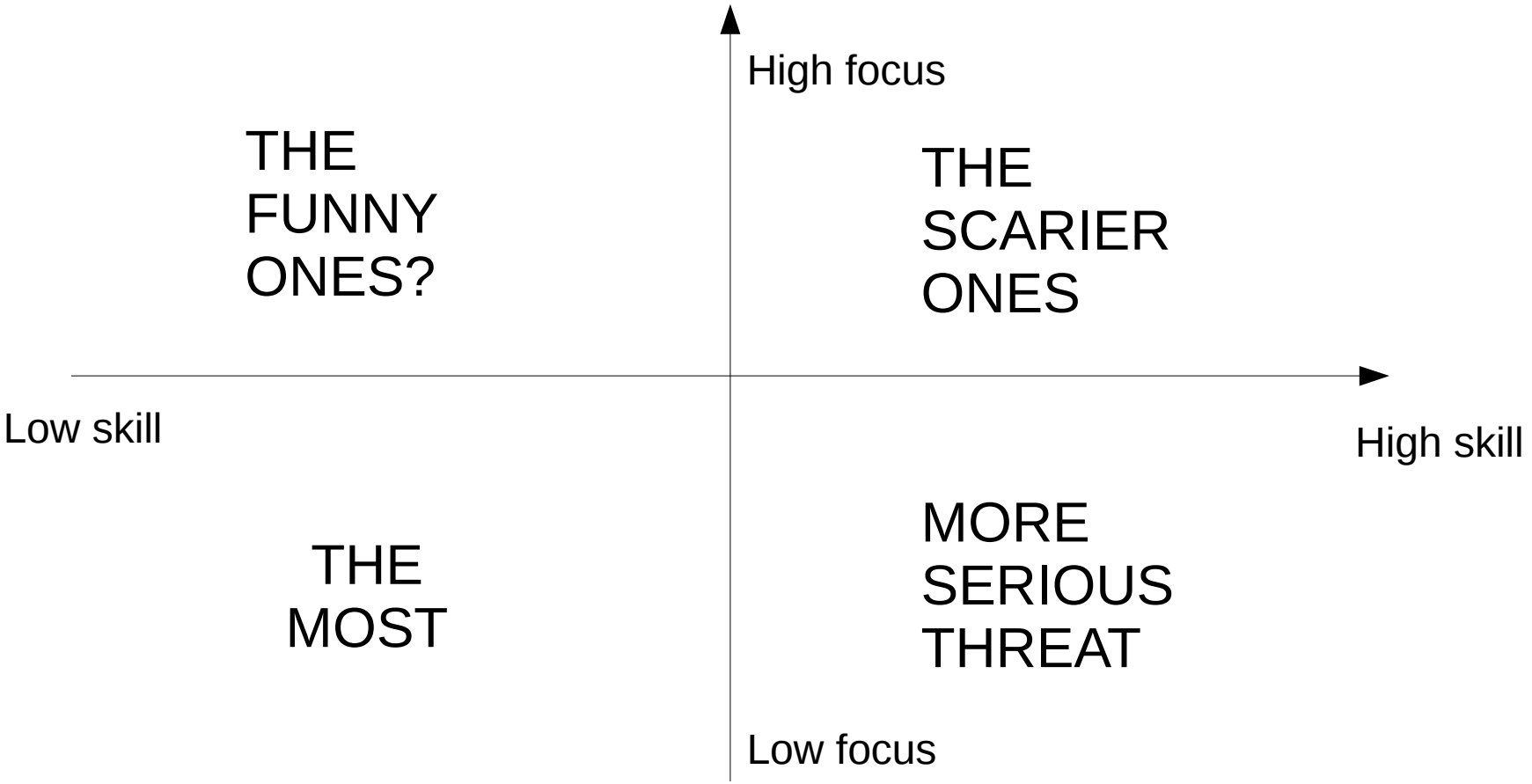


Based on Lockheed Martin's Cyber Kill Chain

Threats in cyberspace

Threat actors

- By skills and focus



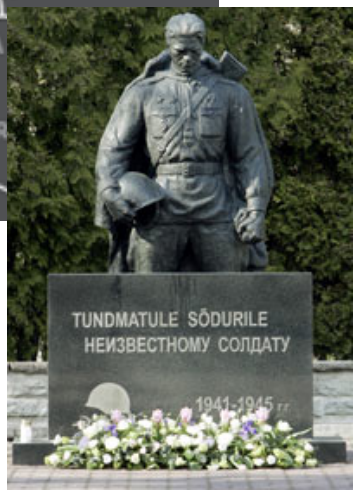
Cyber war

Cyber war

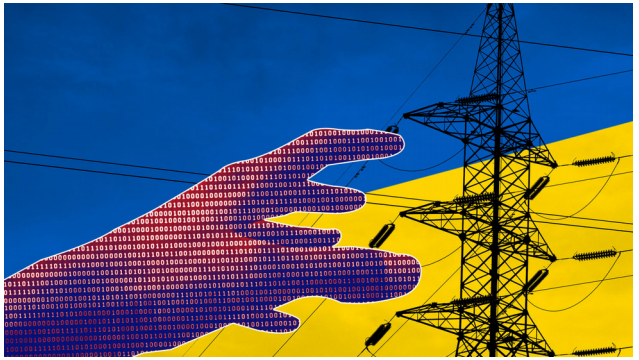
“Actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption.”

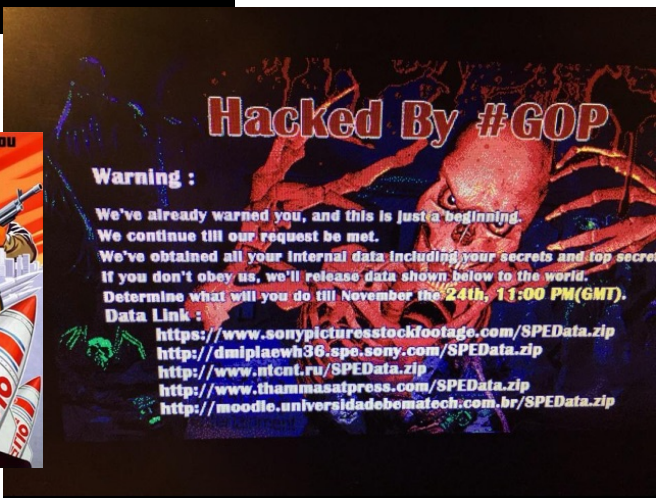
- Richard A. Clarke, former Special Advisor to the US President on cyber security, in “Cyber War” (Harper Collins, 2010)

Cyber war

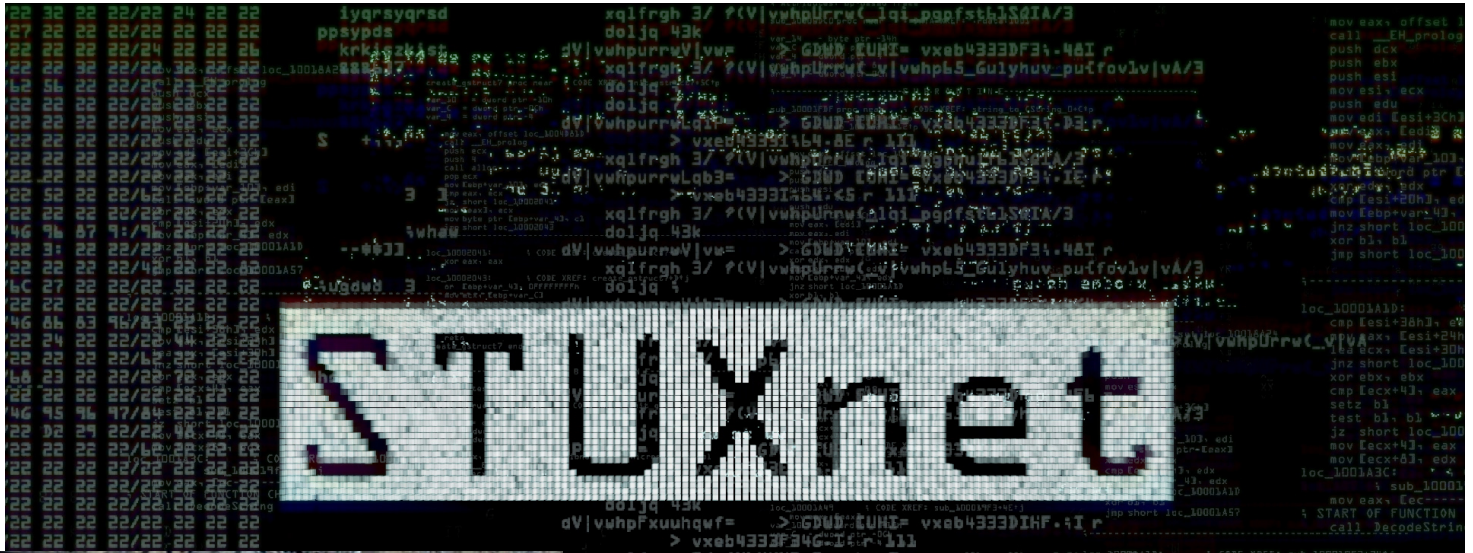


SONY





Stuxnet


STUXnet


Underground structure, under construction, intended as a support building for the two cascade buildings
Underground structures, under construction, intended to house gas centrifuge cascades
Thick Wall
Centrifuge Assembly Area
Underground Truck Road
Tunnel Entrance
Administration Building
Image: DigitalGlobe/Annotation: ISIS
Image Date: September 16, 2002

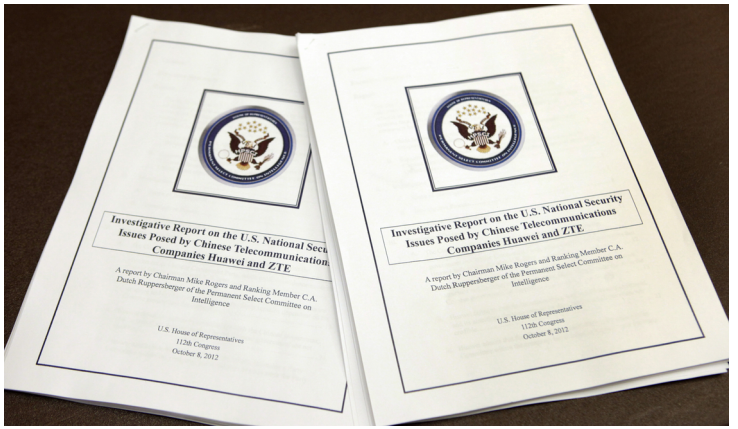
Cyber terrorism

Cyber terror

- Terror: the use of intentionally indiscriminate violence as a means to create terror, or fear, to achieve a political, religious or ideological aim
- Cyber terror: same, just in cyber space

Sypply chain threats

Supply chain threats



Hacktivism

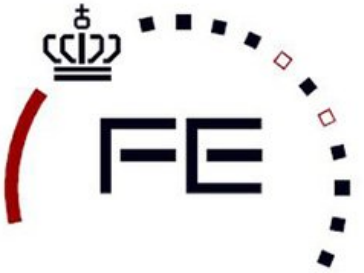
Hacktivism


ASHLEY
MADISON®.COM


Hacked Team
@hackingteam
Follow
Since we have nothing to hide, we're publishing all our e-mails, files, and source code mega.co.nz/#!Xx1IhChT!rbB... infotomb.com/eyyxo.torrent
RETWEETS 57
FAVORITES 32
5:26 PM - 5 Jul 2015
© 2015 Twitter About Help Ads info

Cyber espionage

Cyber espionage



Cyber crime

Cyber crime

Offering	Price
1-day DDoS service	US$30-70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

Offering	Price
Linux rootkit that replaces ls, find, grep, and other commands	US$500
Windows rootkit that operates at the driver level and that allows the download of specially assembled drivers	US$292

Lecture plan

- Intro and attacker modus
- **Software** and web app security
- System security
- Cryptography
- Network security
- Reactive security
- Outro