Zero day exploits

UNDERSTANDING THESE EXPLOITS AND THE DANGER THEY PRESENT

Zero Day

About the Speaker

- 20 books (Including 3 on forensics, 5 on computer security, 1 on cryptology)
- Over 40 industry certifications including several forensic certifications
- Member and Diplomat of the American College of Forensic Examiners
- Chair of the cyber forensics board for the American College of forensic Examiners
- 2 Masters degrees and multiple graduate certificates
- 7 Computer science related patents
- Over 25 years experience, over 15 years teaching/training
- Helped create CompTIA Security+, Linux+, Server+. Helped revise CEH v8
- Frequent consultant/expert witness
- Presents workshops talks at security conferences all over the world including Defcon, Hakon India, Hakon Africa, ADFSL, ISC2 Security Congress, Secure World, etc.

www.chuckeasttom.com

chuck@chuckeasttom.com

What is a zero day exploit?

- "A zero-day vulnerability, at its core, is a flaw. It is an unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong. In fact, a zero-day exploit leaves NO opportunity for detection ... at first." – FireEye https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html

Zero Day

What is a zero day exploit?

- "Zero-day refers to how long the "good guys" have known about a security problem in the software. There are two kinds of zero-days. A zero-day vulnerability is a hole in the software's security and can be present on a browser or an application. A zero-day exploit, on the other hand, is a digital attack that takes advantage of zero-day vulnerabilities in order to install malicious software onto a device"
- - Avast https://www.avast.com/c-zero-day

Zero Day

The impact

- Used with increasing sophistication, 0day attacks have been essential in successful Advanced Persistent Threat (APT) style attacks making headlines recently. The problem is evident; incident handlers and response teams struggle to identify and respond to unknown threats.
- -https://www.sans.org/reading-room/whitepapers/incident/responding-zero-day-threats-33709

Zero Day

What happens in the gap?

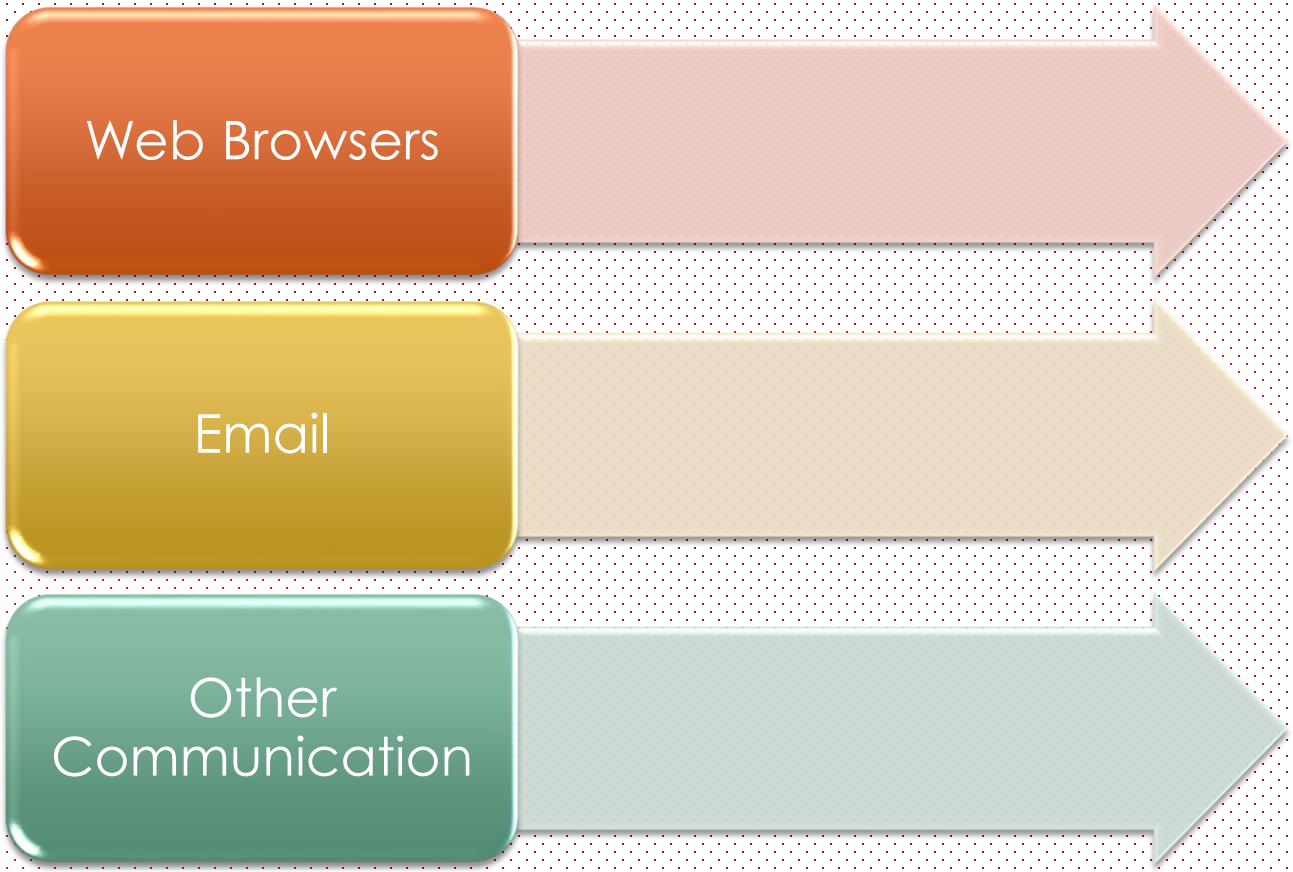
Zero Day

Antivirus and Zero Day

- While they cannot be detected based on signature, how a zero day is exploited may lead to detection. For example, malware exploits might be detected based on behavior. But such detection is far less likely.

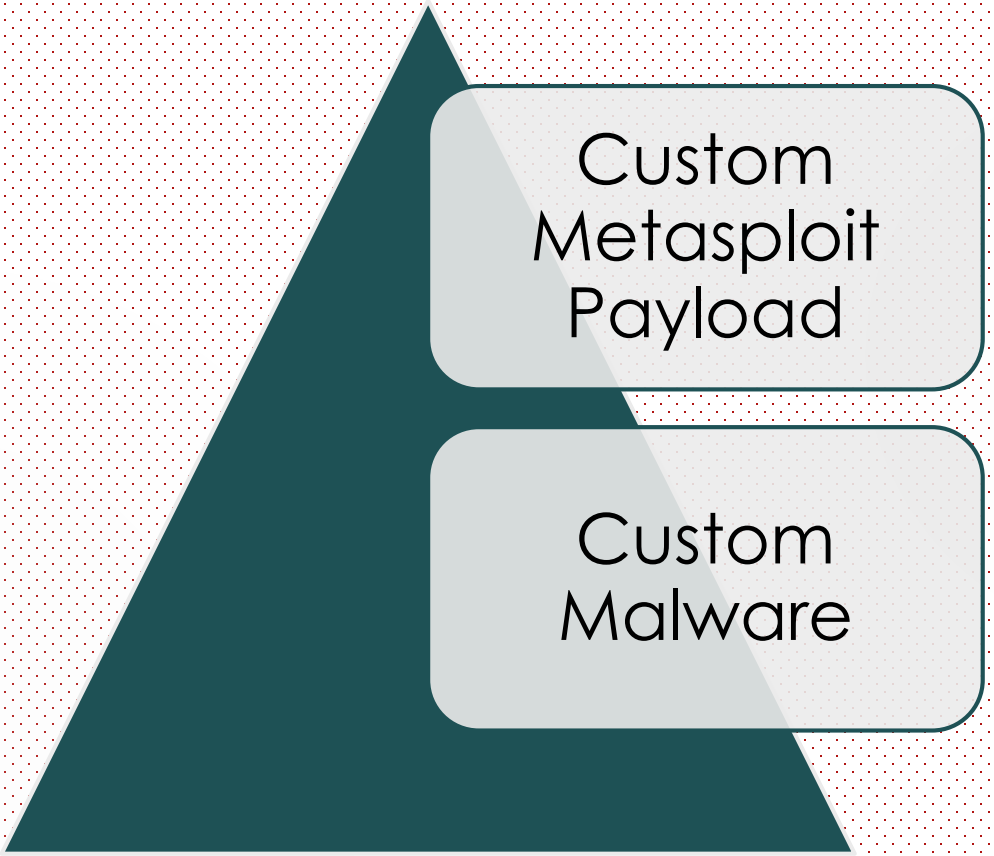
Zero Day

Attack Vectors



Zero Day

How are these exploited



Zero Day

How are these found

- Direct Discovery via Research
- Zero – Day Markets

Zero Day

Zero Day Market Types

- White
- Gray
- Black

Zero Day Market Details

White markets typically reward people who find flaws and pay in cash/check

Black/Gray markets don't reveal the discoverer or the purchaser, and pay in bitcoin. Several on the Dark Web.

Finding a vulnerability can be a commodity, but a more valuable commodity (particularly on the black market) is software that can actually exploit the vulnerability.

This is part of the growing cyber-arms industry

Zero Day Market Details

Exploit vendor Zerodium has tripled its bug bounty for an Apple's iOS 10 zero-day exploit, offering a maximum payout of $US1.5 Million.

-http://thehackernews.com/2016/09/zerodium-zero-day-exploit.html

Zero Day Examples

Pegasus is spyware that used three different zero day issues to exploit iOS

“Trident is used in a spyware product called Pegasus, which according to an investigation by Citizen Lab, is developed by an organization called NSO Group. NSO Group is an Israeli-based organization that was acquired by U.S. company Francisco Partners Management in 2010, and according to news reports specializes in “cyber war.” Pegasus is highly advanced in its use of zero-days, obfuscation, encryption, and kernel-level exploitation”
-https://blog.lookout.com/blog/2016/08/25/trident-pegasus/

Zero Day Examples

In April of 2016 cybersecurity experts found an exploit based on this vulnerability for sale on a darknet marketplace where the seller was asking around $15,000. In July, the first malware appeared that used this vulnerability. This piece of malware, the Dyre Banking Trojan, targeted users all over the world and was designed to steal credit-card numbers from infected computers.

Zero Day Examples

In September 2016 a MySQL Zero Day Exploit was disclosed

"The flaw, tracked as CVE-2016-6662, can be exploited to modify the MySQL configuration file (my.cnf) and cause an attacker-controlled library to be executed with root privileges if the MySQL process is started with the mysqld_safe wrapper script."

http://www.infoworld.com/article/3119120/security/mysql-zero-day-exploit-puts-some-servers-at-risk-of-hacking.html

Zero Day

Zero Day Examples

In October 2016 Digital Defense, Inc. (DDI), a leading provider of Vulnerability Management as a Service (VMaaS™), disclosed the discovery of four security vulnerabilities found in the Dell SonicWALL Email Security virtual appliance application.

DDI detected the previously unknown vulnerabilities while developing new audit modules for its patented vulnerability scanning technology. The vulnerabilities can lead to leaking the administrative account password hash, allowing command execution as root, and a full compromise of the appliance.

Zero Day

Counter measures

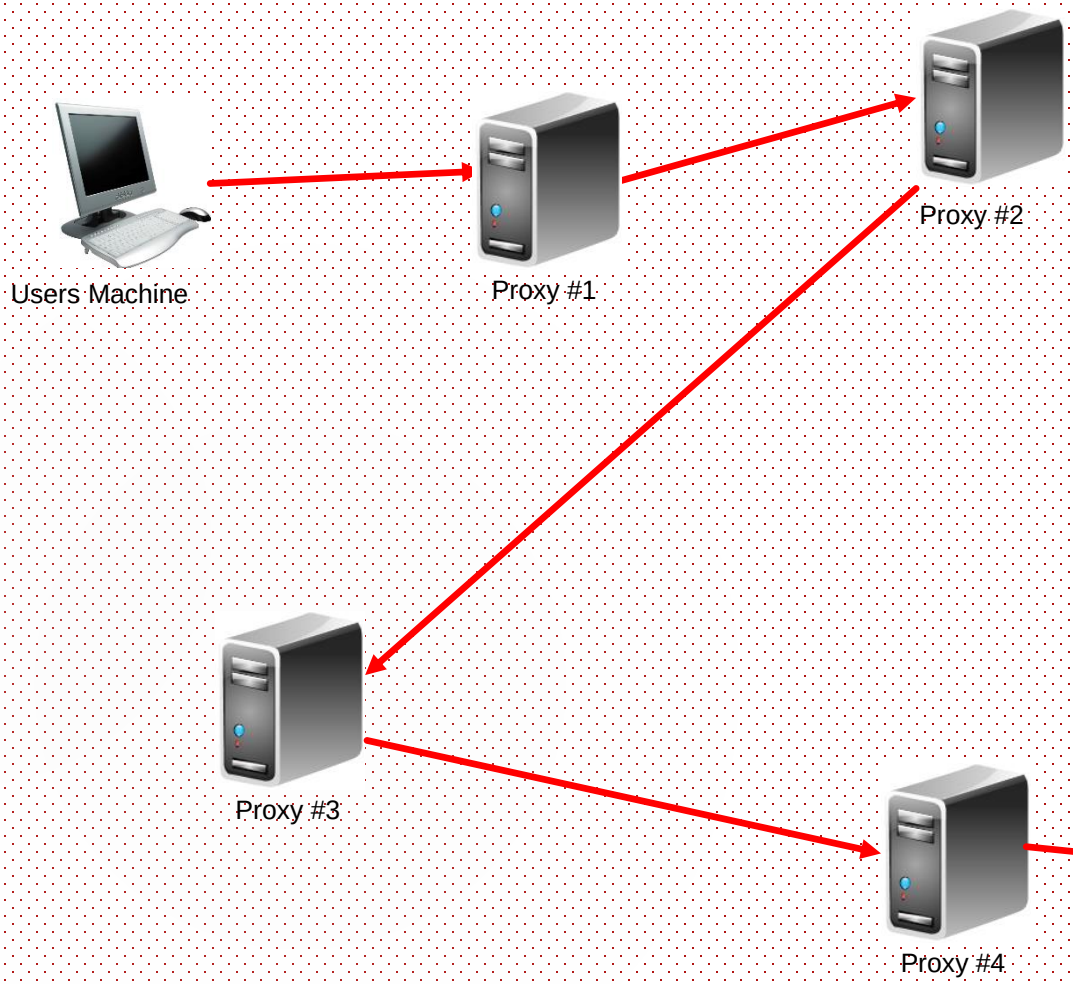
Zero days are often sold on the dark web

MIT has published a description of a machine based search of dark web markets that identified over 300 cyber threats each weak. It is essentially an automated web crawler looking for zero day exploits for sale on the dark web.

Tor Networks

TOR, https://www.torproject.org/, is an anonymous network of proxy servers. One can use the TOR network to send any sort of network traffic, including emails. This makes tracing the traffic back to its source extremely difficult.

Accessing a website VIA TOR



Each proxy just sends the packet on and only knows the last and next hop.

The path can change each route

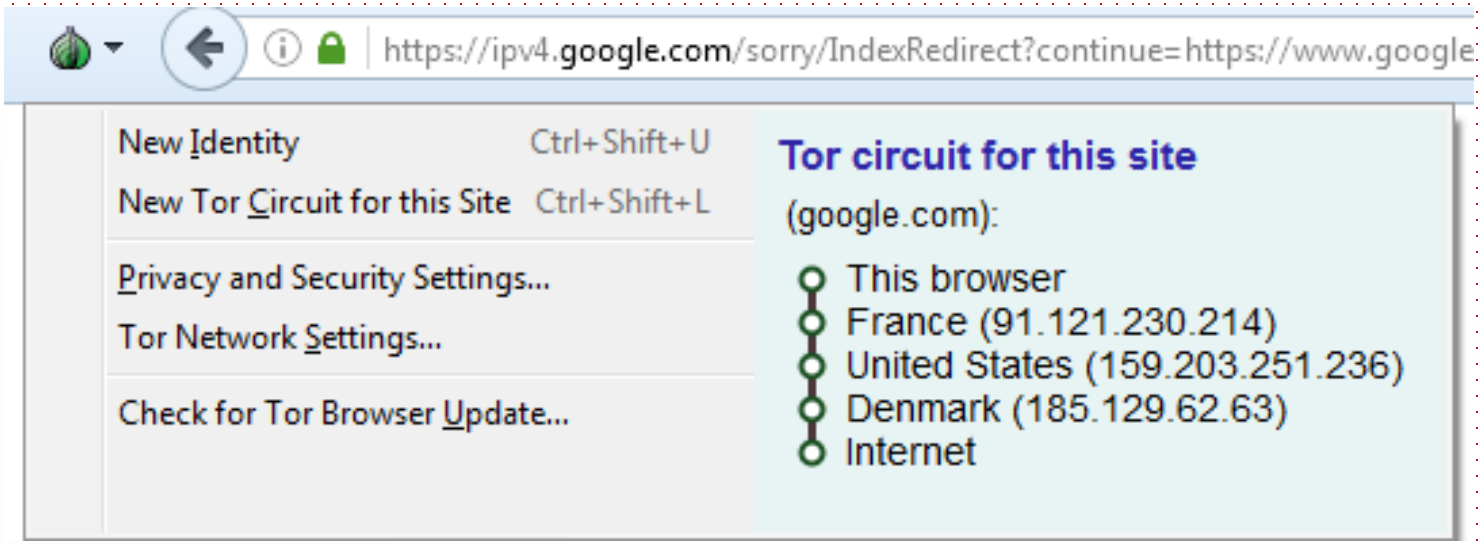
The target server only knows the last hop the packet came from

The user only knows the first proxy in the chain

Zero Day

The result

- Using a TOR browser from my house in Plano Texas, I am actually surfing the web as if I were in Denmark

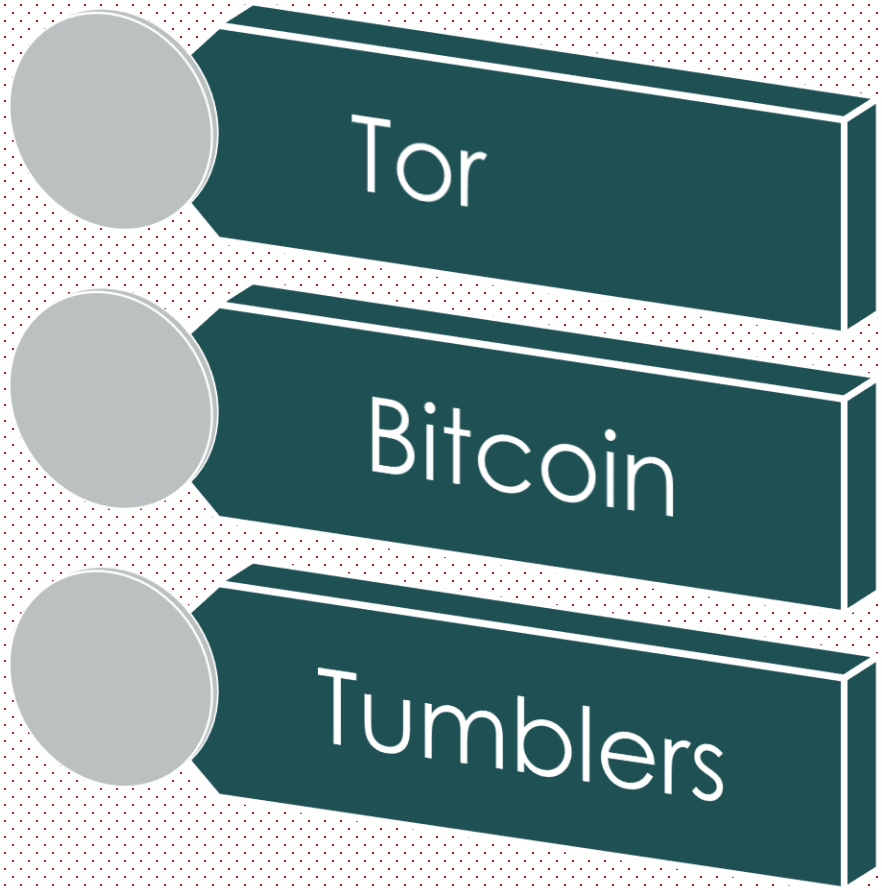


The Dark Web

- Hidden and only accessible via Tor networks.
- Also called the dark net
  - Note: many people use the term deep web not to refer to the dark web, but rather to normal websites not indexed by search engines.
- Not only uses, but the servers are hidden via Tor networks. This makes them ideal for privacy advocates as well as for criminals.
- Sites end in .onion

Dark Web Markets

How they work



Hidden/Tor Markets

- Silkroad and Silkroad2 were just the most publicized.
- Many purport to offer
  - Fake ID/Passports
  - Hacking tools
  - Access to botnets
  - Drugs
  - Weapons
  - Malware
  - Zero-day exploits

Zero Day

Questions

www.chuckeasttom.com
chuck@chuckeasttom.com