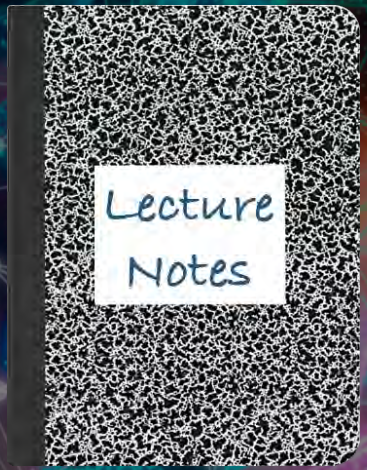
CS 419: Computer Security

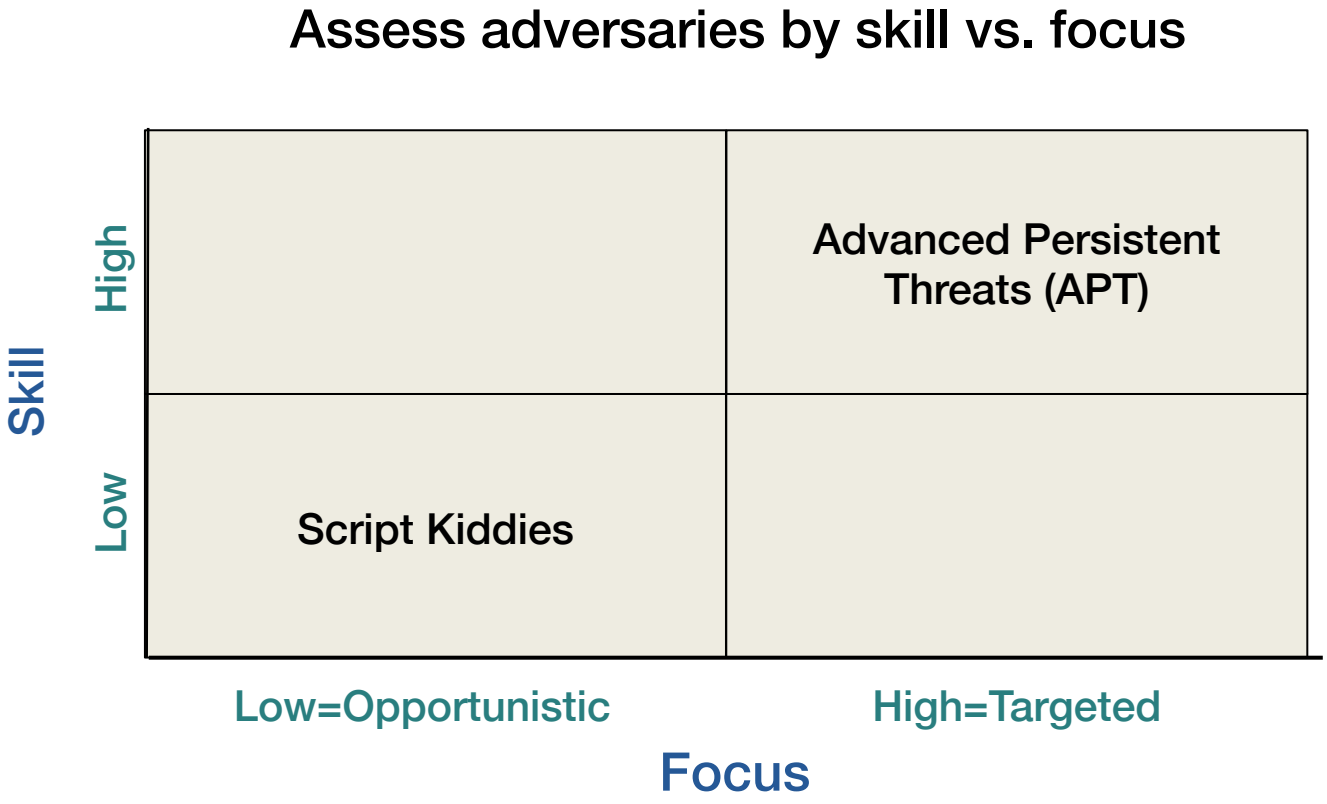
Week 1: Part 4

Attacks & Motives



Paul Krzyzanowski

Threat Matrix



Teen Hacker Charged with Paralyzing Miami Schools in Embarrassingly Simple Cyberattack

GIZMODO

Alyse Stanley • September 5, 2020

A Florida teenager allegedly used an embarrassingly simple program to launch a series of DDoS attacks that helped shut down one of the nation's largest school districts for its first three days of virtual classes, the Miami Herald reported this week.

…

"The student admitted to orchestrating eight Distributed Denial-of-Service cyberattacks, designed to overwhelm district networks," the district said in a statement. More than 345,000 students attend public schools in Miami-Dade County, making it the fourth-largest district in the U.S.

…

Even more embarrassing still, the student admitted that he broke the network using a decade-old, open-source tool that most bare-bones firewall software can catch, the Herald reported Saturday.

The application's called LOIC, which stands for Low Orbit Ion Cannon. Developed by 4Chan-affiliated hackers, it basically did for DDoS attacks what Microsoft Word did for word processors by streamlining the process into an easy-to-download program that even an idiot can't mess up. No hacking experience needed, just point, click, and boom! You're on your way to committing a felony. LOIC makes it easy to coordinate thousands of anonymous users to overwhelm servers by submitting tons of garbage requests en masse.

https://gizmodo.com/teen-hacker-charged-with-paralyzing-miami-schools-in-em-1844968182

Group of unskilled Iranian hackers behind recent attacks with Dharma ransomware

Security firm Group-IB says the hackers have been targeting companies in Russia, Japan, China, and India.

Catalin Cimpanu • August 24, 2020

Cyber-security firm Group-IB says it identified a group of low-skilled hackers operating out of Iran that has been launching attacks against companies in Asia and attempting to encrypt their networks with a version of the Dharma ransomware.

The attacks have targeted companies located in Russia, Japan, China, and India, according to a report Group-IB researchers published Aug. 24.

The security firm described the group as "newbie hackers" based on the low level of sophistication and simple tactics and tools employed during attacks.

Per the report, the group used only publicly-available hacking tools, either open-sourced on GitHub or downloaded from Telegram hacking channels.

This included the likes of Masscan, NLBrute, Advanced Port Scanner, Defender Control, or Your Uninstaller.

https://www.zdnet.com/article/group-of-unskilled-iranian-hackers-behind-recent-attacks-with-dharma-ransomware/

Launching a Ransomware Attack Against Nation Is Far Easier Than You Think

Newsweek

Naveed Jamali, Tom O'Connor, Alex J.. Rouhandeh • July 8, 2021

As ransomware attacks surge to unprecedented levels, the intricacies of mounting such a potentially destructive and deceptive operation would seem to be far beyond the reach of the average netizen.

But the power to paralyze a company or a nation with malicious intent may be more readily available than is commonly thought—although it is illegal, especially for users in the United States.

A U.S. military cyberwarfare officer who spoke to Newsweek on the condition of anonymity described a very simple process for doing a great deal of damage.

"All you need is a Tor Browser and the links to the right underground markets," the officer said. "There's forums, and you can Google them."

…

It's not unlike buying a third-party smartphone application, a pre-packaged bundle of code that enables a device to perform a large range of functions with convenience. And just as consumers can download apps from leading social media companies such as Facebook, Twitter and TikTok, prospective hackers can buy the tools used by top collectives such as REvil.

https://www.newsweek.com/launching-ransomware-attack-against-nation-far-easier-you-think-1608108

"All the News That's Fit to Print"

The New York Times

Late Edition
Today, overcast, breezy, chilly, rain, high 56. Tonight, cloudy, a bit of rain, low 52. Tomorrow, early showers, then some sunshine, warmer, high 67. Weather map is on Page 26.

VOL. CLXX ... No. 59,074 NEW YORK, SUNDAY, MAY 30, 2021 $6.00

From Russians, Ransomware, Made to Order

This article is by Andrew E. Kramer, Michael Schwirtz and Anton Troianovski.

MOSCOW — Just weeks before the ransomware gang known as DarkSide attacked a major American pipeline, disrupting gasoline and jet fuel deliveries up and down the East Coast of the United States, the group was turning the screws on a small, family-owned publisher based in the American Midwest.

Working with a hacker who went by the name of Woris, DarkSide launched a series of attacks meant to shut down the websites of the publisher, which works mainly with clients in primary school education, if it refused to meet a $1.75 million ransom demand. It even threatened to contact the company's clients to falsely warn them that it had obtained information the gang said could be used by pedophiles to make fake identification cards that would allow them to enter schools.

Woris thought this last ploy was a particularly nice touch.

"I laughed to the depth of my soul about the leaked IDs possibly being used by pedophiles to enter the school," he said in Russian in a secret chat with DarkSide obtained by The New York Times. "I didn't think it would scare them that much."

DarkSide's attack on the pipeline owner, Georgia-based Colonial Pipeline, did not just thrust the gang onto the international stage. It also cast a spotlight on a rapidly expanding criminal industry based primarily in Russia that has morphed from a specialty demanding highly sophisticated hacking skills into a conveyor-belt-like process. Now, even

Continued on Page 14

The different characteristics of attackers

- Goals
- Levels of access
- Risk tolerance
- Resources
- Expertise
- Economics

Who are the adversaries?

- **Hackers**
  - Good or evil
    - White hat hackers: do not intend to cause damage; goal = profit or fixing bugs
    - Black hat hackers: profit by hacking or selling services to the highest bidder
  - Test boundaries of the system – get to know the system better than designers
  - Only a small % are smart
  - Bug hunters – find vulnerabilities
  - Exploit writers – write code to exploit the vulnerabilities
- **Criminals**
  - Individuals or small groups
  - Don’t necessarily reap huge $ but are often creative

Who are the adversaries?

- **Malicious insiders**
  - Insidious because they are indistinguishable from legitimate, trusted insiders
  - Perimeter defenses don't work
  - Often have high levels of access
- **Industrial spies**
  - Product designs, trade secrets, project bids, finances, employee info
  - Can hire/bribe employees to reveal trade secrets or become inside attackers
  - … or resort to dumpster diving
  - Risk-averse: reputation of company (or country) damaged if caught

https://www.idwatchdog.com/insider-threats-and-data-breaches

Who are the adversaries?

- **Press (& politicians)**
  - Social engineering, bribing, dumpster diving, track movements, eavesdrop, break in
  - Also generally risk averse for fear of losing one's reputation & career
- **Organized crime**
  - More opportunities to make or launder money!
  - Money laundering is easier with EFT and cryptocurrency

Organized Crime

Example: Russian Business Network (RBN)

- **Operates on numerous ISPs worldwide**
- **Internet service provider run by criminals for criminals**
  - Host platform for illegal businesses
- **Domains registered to anonymous addresses**
  - Does not advertise
  - Trades in untraceable electronic transactions
- **Known for delivering fake anti-spyware & anti-malware software**
  - Used for PC hijacking and personal identity theft
- **One of the world's worst spammer, malware, and phishing networks**

Who are the adversaries?

- **Police**
  - Risk averse but have law on their side (e.g., search warrants, seizing evidence)
  - Not above breaking law: wiretaps, destruction of evidence, disabling body cameras, illegal search & seizure
- **Hacktivists, Terrorists (freedom fighters)**
  - Motivated by geopolitics, religion, or a set of ethics
  - Examples: Earth First, Hezbollah, ISIS, Aryan Nations, Greenpeace, and PETA
  - Usually more concerned with causing harm than getting specific information
  - Usually (not always) low budgets & low skill levels
  - Have grown more sophisticated lately
    - Ukrainian IT Army vs. Russia's KillNet group
    - Israel-Palestine website and DDoS attacks

Hacktivist Group Leaks Disney's Slack Channels Over its Stance on AI Images

PetaPixel

Matt Growcoot • July 17, 2024

A group of hacktivists has leaked over a terabyte of data from Disney's internal communications platform over the company's stance on AI imagery.

The group called NullBulge released the data from Disney's Slack channels yesterday through a peer-to-peer network. It says it is motivated to "protect artists' rights and ensure fair compensation for their work".

That is different from a hacker's usual modus operandi who often demand ransoms. NullBulge leaked the dossier of photos, converstations, and unreleased projects quite quickly saying that making demands from Disney would be futile.

https://petapixel.com/2024/07/17/hacktivist-group-leaks-disneys-slack-channels-over-its-stance-on-ai-images/

Who are the adversaries?

- **National intelligence organizations**
  - Huge money & long-term goals
  - Somewhat risk averse
    - Bad public relations
    - Do not want leaks to reveal attack techniques
  - Often have a lot of influence
    - NSA was instrumental in the adoption of 56-bit keys for DES or the Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator)
    - Lenovo computers, owned partially by the Chinese government's Academy of Sciences has been accused of "malicious circuits" built into the computers
    - NSA planted backdoors into Cisco routers built for export that allows the NSA to intercept any communications through those routers.
- **Nation-states: Infowarriors, cyber warfare**
  - Huge money & short-term goals
  - Disrupt power grids, commerce, transportation
  - EMP weapons, spread selective information, misinformation, blackmail

Cyber Warfare:
Nation State Attacks

Microsoft notified 10,000 victims of nation-state attacks

Most of the attacks came from state-sponsored hacking groups in Iran, North Korea, and Russia.

By Catalin Cimpanu for Zero Day | July 18, 2019

Microsoft said that over the past year it notified nearly 10,000 users that they'd been targeted or compromised by nation-state hacking groups.

The company didn't just blast out random statistics, but also named names. Microsoft said most of the attacks came from state-sponsored hackers from Iran, North Korea, and Russia.

More precisely, the Iran attacks came from groups Microsoft calls Holmium and Mercury, the North Korean attacks came from a group called Thallium, and the Russian attacks came from groups called Yttrium and Strontium.

https://www.zdnet.com/article/microsoft-notified-10000-victims-of-nation-state-attacks/

A Growing Army of Hackers Helps Keep Kim Jong Un in Power

Bloomberg

North Korea relies on cybercrime to fund its nuclear arms program and prop up the ailing economy.

Jon Herskovitz & Jeong-Ho Lee • December 21, 2021

Kim Jong Un marked a decade as supreme leader of North Korea in December. Whether he can hold on to power for another 10 years may depend on state hackers, whose cybercrimes finance his nuclear arms program and prop up the economy.

According to the U.S. Cybersecurity & Infrastructure Security Agency, North Korea's state-backed "malicious cyberactivities" target banks around the world, steal defense secrets, extort money through ransomware, hijack digitally mined currency, and launder ill-gotten gains through cryptocurrency exchanges. Kim's regime has already taken in as much as $2.3 billion through cybercrimes and is geared to rake in even more, U.S. and United Nations investigators have said.

The cybercrimes have provided a lifeline for the struggling North Korean economy, which has been hobbled by sanctions. Kim has shown little interest in returning to negotiations that could lead to a lifting of sanctions if North Korea winds down its nuclear arms program.

Money from cybercrimes represents about 8% of North Korea's estimated economy in 2020, which is smaller than when Kim took power, according to the Bank of Korea in Seoul.

https://www.bloomberg.com/news/articles/2021-12-21/north-korean-army-of-cybercriminals-props-up-kim-s-nuclear-program-and-economy

Inside Operation Diplomatic Specter: Chinese APT Group's Stealthy Tactics Exposed

The Hacker News

Ravie Lakshmanan • May 23, 2024

Governmental entities in the Middle East, Africa, and Asia are the target of a Chinese advanced persistent threat (APT) group as part of an ongoing cyber espionage campaign dubbed Operation Diplomatic Specter since at least late 2022.

"An analysis of this threat actor's activity reveals long-term espionage operations against at least seven governmental entities," Palo Alto Networks Unit 42 researchers Lior Rochberger and Daniel Frank said in a report shared with The Hacker News.

"The threat actor performed intelligence collection efforts at a large scale, leveraging rare email exfiltration techniques against compromised servers."

…

Targets of the attacks include diplomatic and economic missions, embassies, military operations, political meetings, ministries of targeted countries, and high-ranking officials.

https://thehackernews.com/2024/05/inside-operation-diplomatic-specter.html

More than half of foreign cyberattacks against China in 2019 originated in the US, China report says

South China Morning Post

China recently tightened its cybersecurity rules, requiring “critical information infrastructure” to undergo a more rigorous review process

Coco Feng • August 12, 2020

More than half of computer malware attacks in China from overseas entities in 2019 originated in the US, according to data from a government-affiliated cybersecurity team.

The total amount of computer malware attacks captured by the National Computer Network Emergency Response Technical Team (CNCERT) was over 62 million in 2019, and around 53.5 per cent of foreign attacks were from the US, lower than a year before when there were in excess of 100 million incidents, the Team said.

Russia and Canada were the second and third largest contributors to computer malware attacks against China, accounting for 2.9 and 2.6 per cent respectively of the total number of foreign attacks.

The number of new malicious attacks directed against mobile networks was nearly 2.8 million in 2019, 1.4 per cent lower than a year earlier, the first decline in such attacks in five years, according to CNCERT.

https://www.scmp.com/tech/policy/article/3097070/more-half-foreign-cyberattacks-against-china-2019-originated-us-china

U.S. Escalates Online Attacks on Russia's Power Grid

The New York Times

By David E. Sanger and Nicole Perlroth • June 15, 2019

The United States is stepping up digital incursions into Russia's electric power grid in a warning to President Vladimir V. Putin and a demonstration of how the Trump administration is using new authorities to deploy cybertools more aggressively, current and former government officials said.

In interviews over the past three months, the officials described the previously unreported deployment of American computer code inside Russia's grid and other targets as a classified companion to more publicly discussed action directed at Moscow's disinformation and hacking units around the 2018 midterm elections.

Advocates of the more aggressive strategy said it was long overdue, after years of public warnings from the Department of Homeland Security and the F.B.I. that Russia has inserted malware that could sabotage American power plants, oil and gas pipelines, or water supplies in any future conflict with the United States.

https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

Stuxnet – 2010, U.S. & Israel (?)

- **Targeted centrifuges used to purify uranium in Iran**
- **Attacked Siemens centrifuges via a SCADA interface**
  - Phase 1
    - Possible initial installation via thumb drive
      Air gapped systems – systems physically separated from other networks
    - Propagated among Microsoft Windows Systems
    - Searched for systems running Siemens Step7 control software
  - Phase 2
    - Altered the spin of the centrifuges while making it look like everything was fine
- **Showed that cyber attacks can cause real-world damage**
- **Pipelines, electric grids, banking, … are at risk**

Regin – 2003(?), U.S.(?)

- **Reputed to be the most advanced malware & hacking toolkit**
- **Developed by the NSA & GCHQ (maybe)**
- **Modular design – goal is to stay hidden and collect information**
- **Target**
  - Individuals, telecom, energy, hospitality, and research companies
  - Surveillance on European Union citizens and companies

Shamoon – 2012, Iran

- **Developed by Iran's state hackers (allegedly)**
- **Deployed in 2012 on the network of Saudi Aramco**
  - Wiped data on over 30,000 computers
  - Deployed again in 2016
- **2018: attacked computers of Saipem, an Italian oil & gas company**
  - Infected about 10% of the company's systems

Some Nation-State Attacks (probably)

- **2015: First known successful cyber attack on a power grid (Russia against Ukraine)**
  - 30 substations were switched off and 230,000 people were without power for 1-6 hours
  - Attacks carried out from computers with Russian IP addresses
- **2018 and earlier: Russian accesses U.S. infrastructure (Russia against U.S.)**
  - Russian hackers had direct access to an American power company's control systems
  - Lays groundwork for future attacks
- **2017: NotPetya malware attacks on Ukraine and other regions (Russia against Ukraine)**
  - >$10B damages
  - Banks, ministries, newspapers, and electricity firms affected
  - Originated from an update to a Ukrainian tax accounting package called MeDoc

https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

Hackers Bring Down Government Sites in Ukraine

The New York Times

A cyberattack defaced the Foreign Ministry website with a message saying "Be afraid," a day after the latest round of talks between Moscow and the West aimed at forestalling a Russian invasion.

Andrew Kramer • January 14, 2022

KYIV, Ukraine — Hackers brought down several Ukrainian government websites on Friday, posting a message on the site of the Foreign Ministry saying, "Be afraid and expect the worst." It was the latest in a long line of cyberattacks targeting the country amid its conflict with Russia.

The attack on Friday was ominous for its timing, coming a day after the apparent breakdown of diplomatic talks between Russia and the West intended to forestall a threatened Russian invasion of Ukraine. The message appeared in Ukrainian, Russian and Polish on the foreign ministry website.

"As a result of a massive cyber attack, the websites of the Ministry of Foreign Affairs and a number of other government agencies are temporarily down," the ministry said in a statement.

Diplomats and analysts have been anticipating a cyberattack on Ukraine, but proving such actions is notoriously difficult. Ukraine did not directly blame Russia for the attack, but pointedly noted that there was a long record of Russian online assaults against Ukraine.

https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html

Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says

FBI

Partnerships, joint operations, and private sector vigilance can help us fight back

April 18, 2024

FBI Director Christopher Wray on April 18 warned national security and intelligence experts, as well as students, that risks the government of China poses to U.S. national and economic security are “upon us now”—and that U.S. critical infrastructure is a prime target.

…

But the CCP also wants to prevent the United States from being able to get in the way of a potential future “crisis between China and Taiwan by 2027,” he said. Americans are starting to feel the effects of this sprint, he said, pointing to “cyber intrusions and criminal activity” as early deterrence efforts by the CCP.

…

Similarly, he said, during the FBI’s recent Volt Typhoon investigation, the Bureau found that the Chinese government had gained illicit access to networks within America’s “critical telecommunications, energy, water, and other infrastructure sectors.” But, he noted, the CCP has also targeted critical infrastructure organizations through more “scattershot, indiscriminate cyber campaigns” that also impact other victims—such as their Microsoft Exchange hack in 2021, which "targeted networks across a wide range of sectors.”

https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says

Are our intelligence efforts secure?

Government agencies try to develop – and pay for – the best attacking & defense techniques

But…

The American Military Sucks at Cybersecurity

A new report from US military watchdogs outlines hundreds of cybersecurity vulnerabilities.

Matthew Gault • January 23, 2019

The Department of Defense is terrible at cybersecurity. That's the assessment of the Pentagon's Inspector General (IG), who did a deep dive into the American military's ability to keep its cyber shit on lockdown. The results aren't great. "As of September 30, 2018, there were 266 open cybersecurity-related recommendations, dating as far back as 2008," the Inspector General said in a new report.

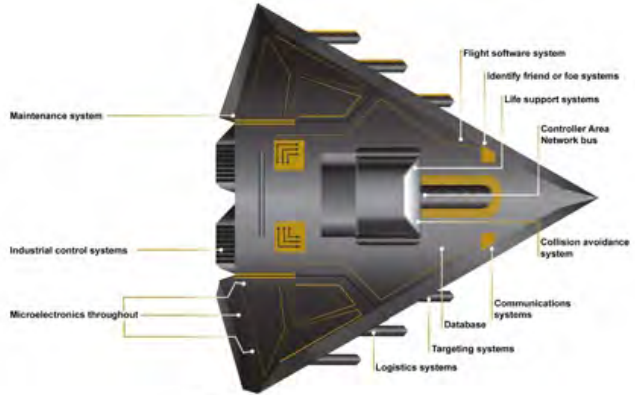
The new report is a summary of the IG's investigations into Pentagon cybersecurity over the previous year. It looked at 20 unclassified and four classified reports that detailed problems with cybersecurity and followed up to see if they'd been addressed. Previously, the IG had recommended the Pentagon take 159 different steps to improve security. It only took 19 of them.

https://motherboard.vice.com/en_us/article/7xy5ky/the-american-military-sucks-at-cybersecurity

BLEEPINGCOMPUTER

US Advanced Weaponry Is Easy to Hack, Even by Low-Skilled Attackers

By Ionut Ilascu • October 9, 2018



Major weapon systems developed by the US Department of Defense are riddled with vulnerabilities that make them an easy target for adversaries trying to control them or disrupt their functions.

As the DoD plans to spend about $1.66 trillion to advance its weapons arsenal, the US Government of Accountability Office (GAO) finds reports from various development stages of the systems showing that mission-critical vulnerabilities are a regular find in "nearly all weapon systems that were under development."

Testing teams charged with probing the resilience to cyber attacks were able to take control or disable the target using basic tools and techniques. Sometimes, just scanning the system caused parts of it to shut down.

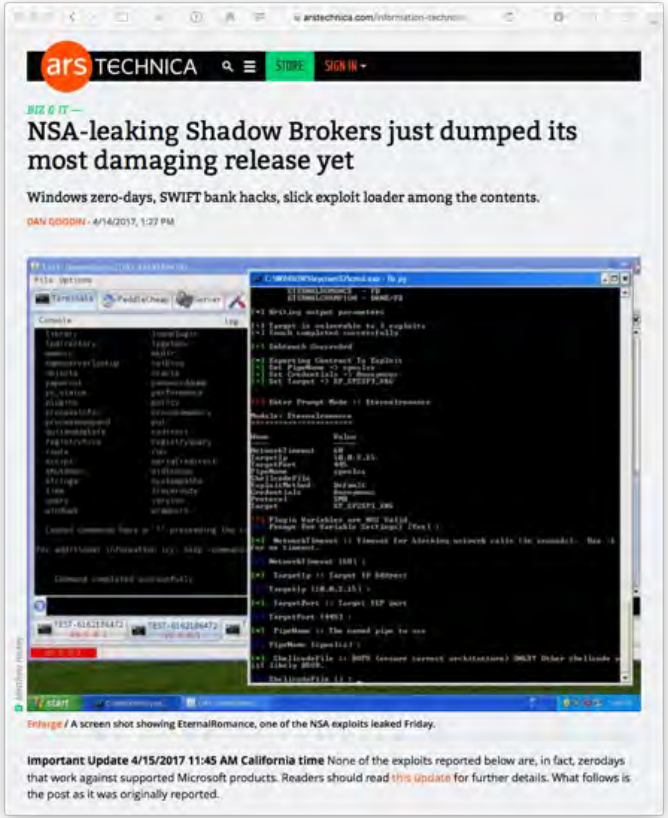
https://www.bleepingcomputer.com/news/security/us-advanced-weaponry-is-easy-to-hack-even-by-low-skilled-attackers/

March 2017 – Wikileaks publishes CIA Vault 7

- 8,761 documents stolen from the CIA
- Document spying operations & hacking tools
- iOS and Android vulnerabilities
- Bugs in Windows
- Ability to turn some smart TVs into listening devices

April 2017 – Theft from the NSA

- **Shadow Brokers**
  Group that leaked a gigabyte of the National Security Agency's weaponized software exploits over an eight-month period
- **Most vulnerabilities were patched …**
  but lots of systems never get updated



Sept 2017 – TAO tools theft from NSA

- Former NSA contractor stole >50 TB of highly sensitive data
- Includes 75% of hacking tools belonging to NSA's Tailored Access Operations
- *"took NSA materials home so that he could become better at his job"*
- *"Theft came to light during the investigation of a series of NSA-developed exploits that were mysteriously published online by a group calling itself Shadow Brokers."*

arstechnica.com/tech-policy/2017/...

ars TECHNICA STORE SIGN IN

POLICY —

Former NSA contractor may have stolen 75% of TAO's elite hacking tools

Prosecutors reportedly plan to charge Harold T. Martin with espionage.

DAN GOODIN - 2/6/2017, 8:05 PM

On Monday, *The Washington Post* reported one of the most stunning breaches of security ever. A former NSA contractor, the paper said, stole more than 50 terabytes of highly sensitive data. According to one source, that includes more than 75 percent of the hacking tools belonging to the Tailored Access Operations. TAO is an elite hacking unit that develops and deploys some of the world's most sophisticated software exploits.

Attorneys representing Harold T. Martin III have previously portrayed the former NSA contractor as a patriot who took NSA materials home so that he could become better at his job. Meanwhile, investigators who have combed through his home in Glen Burnie, Maryland, remain concerned that he passed the weaponized hacking tools to enemies. The theft came to light during the investigation of a series of NSA-developed exploits that were mysteriously published online by a group calling itself Shadow Brokers.

FURTHER READING
Confirmed: hacking tool leak came from "omnipotent" NSA-tied group

Investigators have floated several theories. One holds that Martin directly provided the tools to the person or group responsible for the leak. An alternate theory is that the leakers obtained the software by hacking Martin. As reported in October, Martin was charged with felony theft of government property and unauthorized removal and retention of classified material. Monday's *Washington Post* article says that prosecutors will likely file charges of "violating the Espionage Act by 'willfully' retaining information that relates to the national defense, including classified data such as NSA hacking tools and operational plans against 'a known enemy' of the United States."

An unnamed US official told the paper that Martin allegedly hoarded more than 75 percent of the TAO's library of hacking tools. It's hard to envision a scenario under which a theft of that much classified material by a single individual would be possible.

When Shadow Brokers appeared in October, it published hundreds of TAO-developed exploits, including one that, for years, had exploited what was then a critical unknown vulnerability in a widely used firewall sold by Cisco Systems. Last month, the person or group said it was shutting down in a post that dumped 61 Windows-formatted binary files. Whether Martin was somehow involved with Shadow Brokers or was a compulsive hoarder working alone, the events underscore serious security lapses inside the NSA.

FURTHER READING
NSA-leaking Shadow Brokers lob Molotov cocktail before exiting world stage

Listing image by National Security Agency

Attack Motives

Attack Motives: Criminal attacks

- **Fraud**
- **Theft (financial)**
- **Scams**
  - Pay $$ and get little or nothing back: pyramid schemes, fake auctions
- **Destruction**
- **Intellectual property theft**
  - Sometimes we want to make data accessible but keep control of its distribution: software, music, movies, photos, books
- **Identity theft**
- **Brand theft**

Attack Motives: Privacy violations

- **Surveillance**
  - Databases
  - Installation of surveillance software
  - Traffic analysis
  - Large-scale surveillance
    - E.g., U.S. NSA's ECHELON, China Skynet

Attack Motives: Finding vulnerabilities is a business

- **Dozens of companies have bug bounty programs**
  - They'll pay you if you find security vulnerabilities or come up with exploits
- **Some companies specialize in acquiring exploits**
  - And sell them to institutions, including government agencies

The Washington Post

The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities

Brian Fung • August 31, 2013

https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/

Apple pays record $100,500 to student who found Mac webcam hack

William Gallagher • January 25, 2022

A cyber security student has shown Apple how hacking its Mac webcams can then also leave devices fully open to hackers, earning him $100,500 from the company's bug bounty program.

Ryan Pickren, who previously discovered an iPhone and Mac camera vulnerability, has been awarded what is believed to be Apple's largest bug bounty payout.

According to Pickren, the new webcam vulnerability concerned a series of issue with Safari and iCloud that he says Apple has now fixed. Before it was patched, a malicious website could launch an attack using these flaws.

In his full account of the exploit, Pickren explains it would give the attacker full access to all web-based accounts, from iCloud to PayPal, plus permission to use the microphone, camera, and screensharing. If the camera were used, however, its regular green light would still come on as normal.

https://appleinsider.com/articles/22/01/25/apple-pays-record-100500-to-student-who-found-mac-webcam-hack?utm_medium=rss

Paying for exploits – supply & demand

Zerodium Expects iOS Exploit Prices to Drop as It Announces Surplus

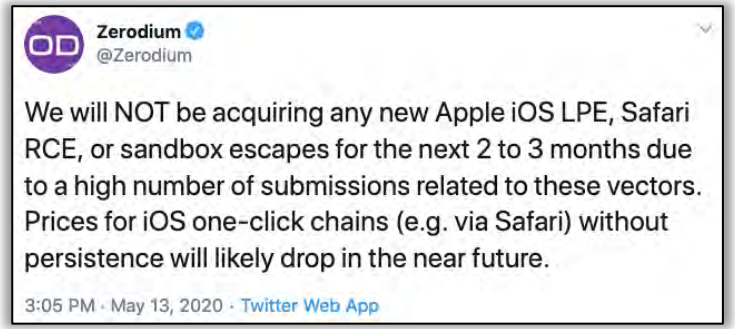
SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Exploit acquisition firm Zerodium announced this week that it's no longer buying certain types of iOS exploits due to surplus, and the company expects prices to drop in the near future.

Eduard Kovacs • May 14 2020

Zerodium said on Twitter it would no longer acquire iOS local privilege escalation, Safari remote code execution, and sandbox escape exploits in the next 2-3 months "due to a high number of submissions related to these vectors."

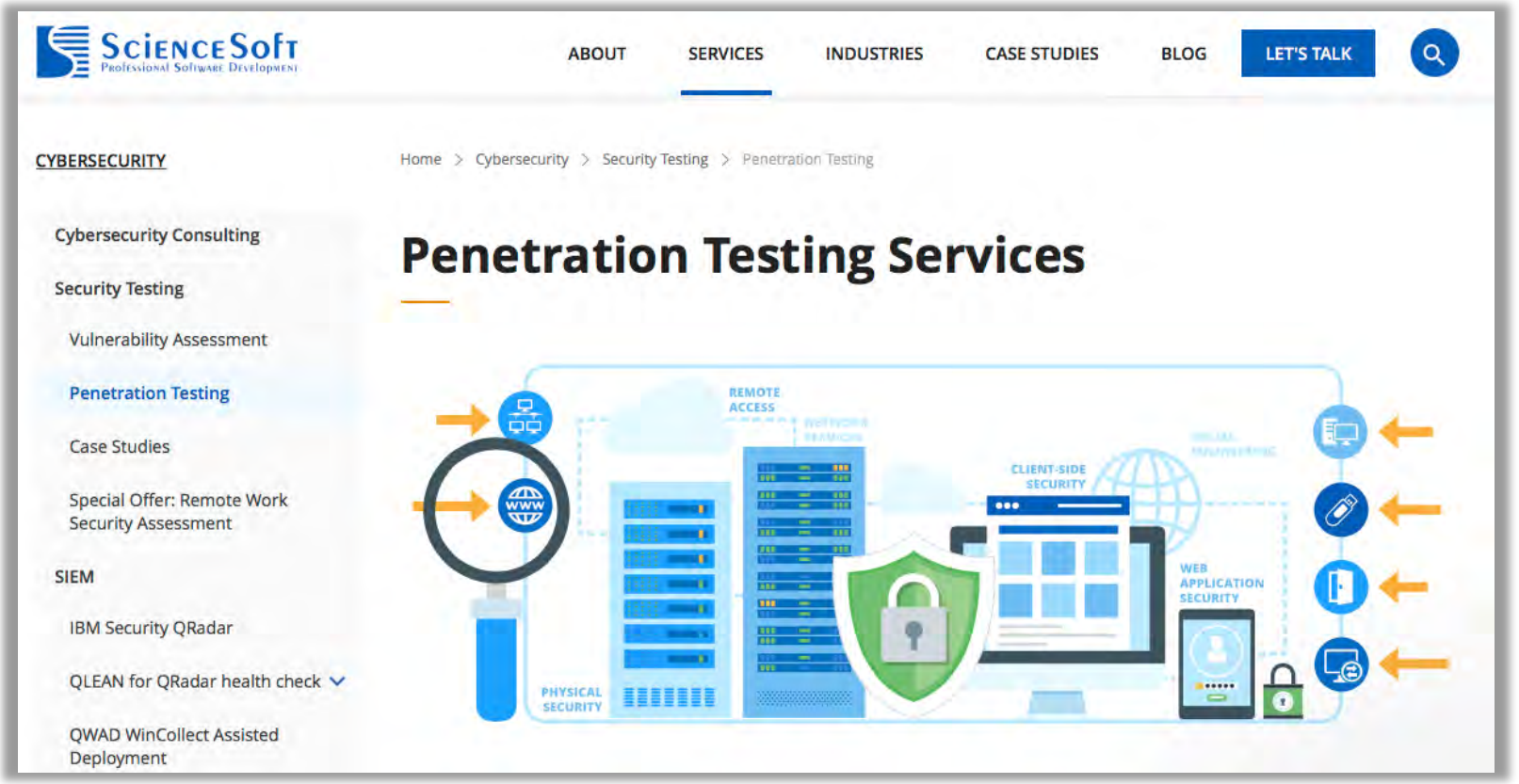
The company says it expects prices to drop for one-click exploit chains that do not provide persistence.



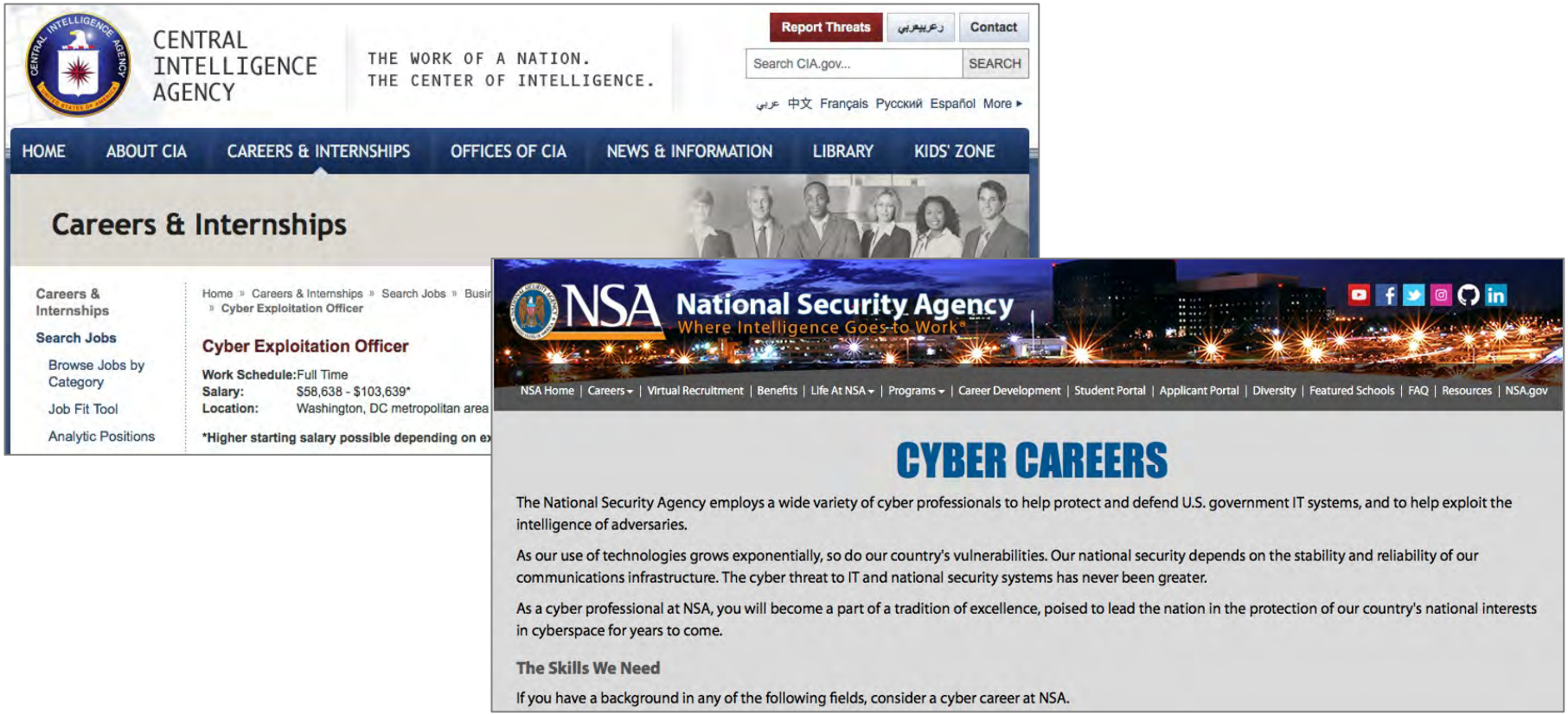
Chaouki Bekrar, CEO and founder of Zerodium, said on Twitter that only pointer authentication codes (PACs) — they provide protection against unexpected changes to pointers in memory — and the difficulty to achieve persistence "are holding [iOS security] from going to zero."

https://www.securityweek.com/zerodium-expects-ios-exploit-prices-drop-it-announces-surplus

Attack Motives: Finding exploits is a career

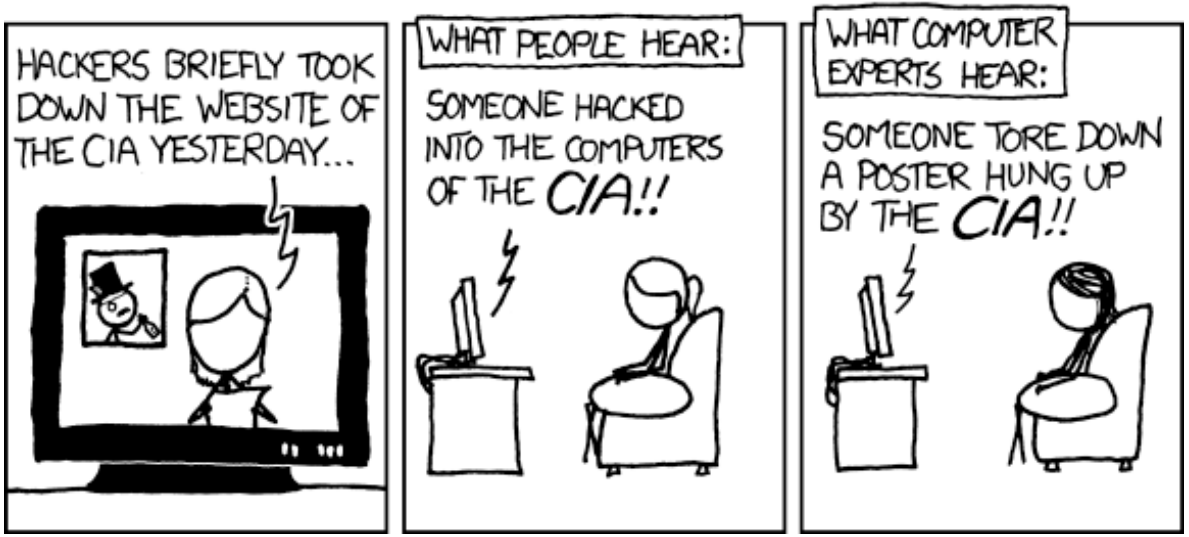


Attack Motives: Building exploits is a career



Other motives

- **Publicity attacks**
- **Availability attacks**
  - Denial of Service (DoS), Distributed Denial of Service (DDoS)



Threat Models

Threat Models

- **Set of assumptions about the abilities of an adversary**
- **A way to identify & prioritize potential threats from an attacker's point of view**
  - Think about things that could go wrong
  - Bad guys don't follow rules: they don't care about your policies
  - We need to understand what types of attacks are possible
- **Assess**
  - What's valuable?
  - Where will you be likely to be attacked?
  - What are the most significant threats?
- **Think about entities in the system, how they communicate & store data**
  - Where are the trust boundaries?
  - Where and how is protection enforced?

Trusted Computing Base

Trusted Computing Base (TCB)

TCB = All hardware & software of a computing system critical to its security

> "The totality of protection mechanisms within it, including hardware, firmware, and software, the combination of which is responsible for enforcing a computer security policy."
>
> – *Orange* Book
> *U.S. Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)*

If the TCB is compromised, we can no longer guarantee the security of a system

Software that is part of the TCB must protect itself against tampering

- Operating system memory protection is an example of this: an application may be compromised but the operating system is still intact and unaffected

Jan 2018 – Meltdown & Spectre

- **Intel chips do not have full memory protection when doing speculative execution**
- **Vulnerability existed for 20 years!**
- **Meltdown**
  - Allows processes to access kernel memory
- **Spectre**
  - Allows processes to steal data from the memory of other processes
- **Also affects ARM & AMD CPUs**

Critical "Meltdown" and "Spectre" Flaws Break Basic Security for Intel, AMD, ARM Computers | WIRED

One of the most basic premises of computer security is isolation: If you run somebody else's sketchy code as an untrusted process on your machine, you should restrict it to its own tightly sealed playpen. Otherwise, it might peer into other processes, or snoop around the computer as a whole. So when a security flaw in computers' most deep-seated hardware puts a crack in those walls, as one newly discovered vulnerability in millions of processors has done, it breaks some of the most fundamental protections computers promise—and sends practically the entire industry scrambling.

Earlier this week, security researchers took note of a series of changes Linux and Windows developers began rolling out in beta updates to address a critical security flaw: A bug in Intel chips allows low-privilege processes to access memory in the computer's kernel, the machine's most privileged inner sanctum. Theoretical attacks that exploit that bug, based on quirks in features Intel has implemented for faster processing, could allow malicious software to spy deeply into other processes and data on the target computer or smartphone. And on multi-user machines, like the servers run by Google Cloud Services or Amazon Web Services, they could even allow hackers to break out of one user's process, and instead snoop on other processes running on the same shared server.

On Wednesday evening, a large team of researchers at Google's Project Zero, universities including the Graz University of Technology, the University of Pennsylvania, the University of Adelaide in Australia, and security companies including Cyberus and Rambus together released the full details of two attacks based on that flaw, which they call Meltdown and Spectre.

"These hardware bugs allow programs to steal data which [is] currently processed on the computer," reads a description of the attacks on a website the researchers created. "While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs."

Popular NPM library hijacked to install password-stealers, miners

BLEEPINGCOMPUTER

Lawrence Abrams • October 23, 2021

Hackers hijacked the popular **`UA-Parser-JS`** NPM library, with millions of downloads a week, to infect Linux and Windows devices with cryptominers and password-stealing trojans in a supply-chain attack.

The UA-Parser-JS library is used to parse a browser's user agent to identify a visitor's browser, engine, OS, CPU, and Device type/model.

The library is immensely popular, with millions of downloads a week and over 24 million downloads this month so far. In addition, the library is used in over a thousand other projects, including those by Facebook, Microsoft, Amazon, Instagram, Google, Slack, Mozilla, Discord, Elastic, Intuit, Reddit, and many more well-known companies.

…

On October 22nd, a threat actor published malicious versions of the UA-Parser-JS NPM library to install cryptominers and password-stealing trojans on Linux and Windows devices.

According to the developer, his NPM account was hijacked and used to deploy the three malicious versions of the library.

https://www.bleepingcomputer.com/news/security/popular-npm-library-hijacked-to-install-password-stealers-miners/

Cisco's warning: Critical flaw in IOS routers allows 'complete system compromise'

Cisco has delivered updates to address four critical flaws affecting its industrial routers.

Liam Tung • June 4 2020

Cisco has disclosed four critical security flaws affecting router equipment that uses its IOS XE and IOS software.

The four critical flaws are part of Cisco's June 3 semi-annual advisory bundle for IOS XE and IOS networking software, which includes 23 advisories describing 25 vulnerabilities.

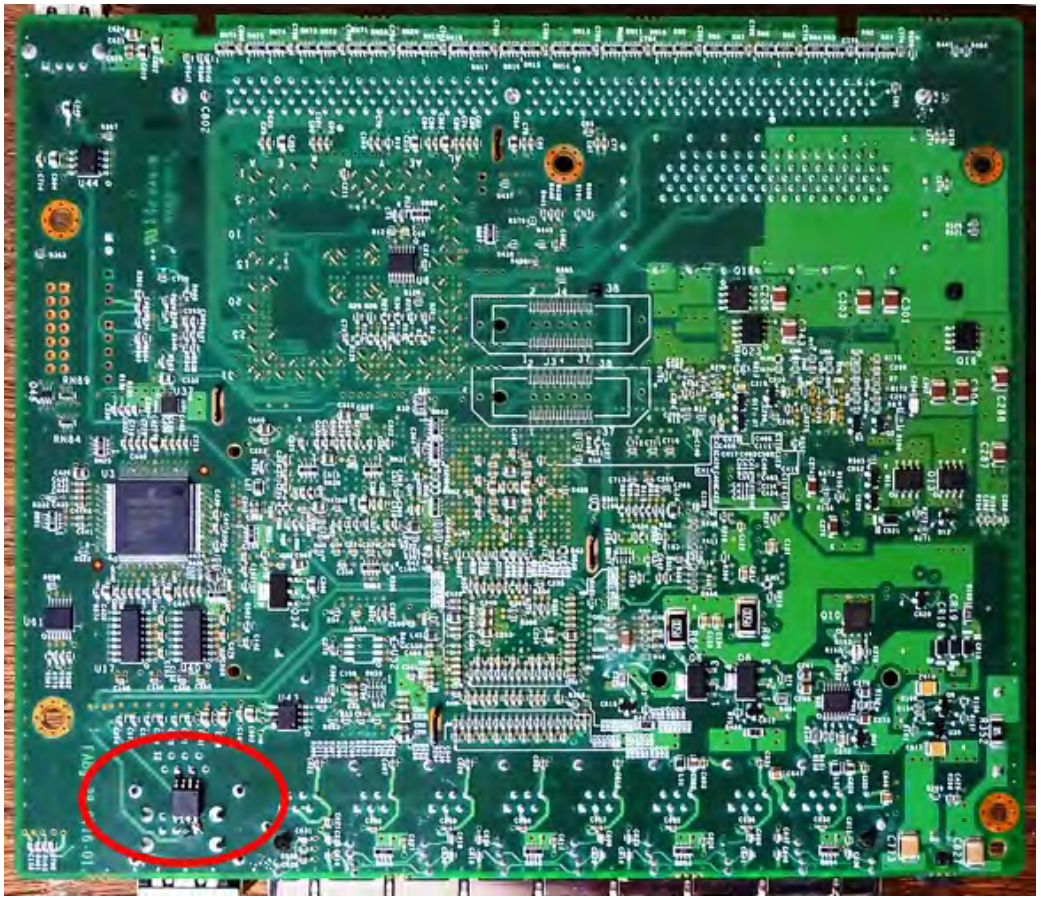
The 9.8 out of 10 severity bug, CVE-2020-3227, concerns the authorization controls for the Cisco IOx application hosting infrastructure in Cisco IOS XE Software, which allows a remote attacker without credentials to execute Cisco IOx API commands without proper authorization.

IOx mishandles requests for authorization tokens, allowing an attacker to exploit the flaw with a specially crafted API call to request the token and then execute Cisco IOx API commands on the device, according Cisco.

https://www.zdnet.com/article/ciscos-warning-critical-flaw-in-ios-routers-allows-complete-system-compromise/

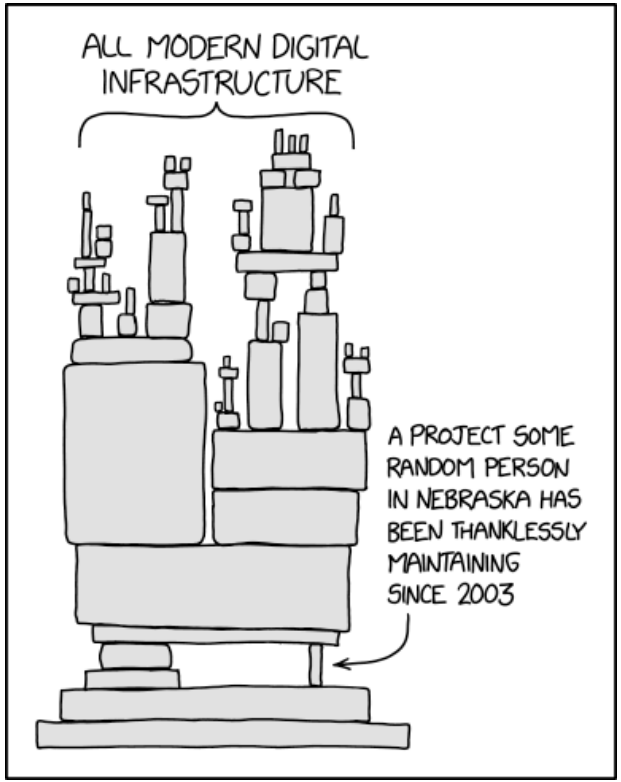
Do you trust the entire supply chain?

- Alter the circuit design
- Add components after the fact
- Modify the CPU
- Modify the bootloader, firmware, or pre-installed software
- Add malware to the compiler used to build the software
- Add malware to libraries used by the apps



Supply chain problems

- **Do you trust every piece of code that is required to run your infrastructure?**
- **Do you know where it comes from?**
- **How actively it's maintained?**
- **Whether it's been audited for vulnerabilities?**



https://xkcd.com/2347/

New UEFI vulnerabilities send firmware devs industry wide scrambling

PixieFail is a huge deal for cloud and data centers. For the rest, less so.

Dan Goodin • January 17, 2024

UEFI firmware from five of the leading suppliers contains vulnerabilities that allow attackers with a toehold in a user's network to infect connected devices with malware that runs at the firmware level.

The vulnerabilities, which collectively have been dubbed PixieFail by the researchers who discovered them, pose a threat mostly to public and private data centers and possibly other enterprise settings. People with even minimal access to such a network—say a paying customer, a low-level employee, or an attacker who has already gained limited entry—can exploit the vulnerabilities to infect connected devices with a malicious UEFI.

Short for Unified Extensible Firmware Interface, UEFI is the low-level and complex chain of firmware responsible for booting up virtually every modern computer. By installing malicious firmware that runs prior to the loading of a main OS, UEFI infections can't be detected or removed using standard endpoint protections. They also give unusually broad control of the infected device.

…

The implementation is incorporated into offerings from Arm Ltd., Insyde, AMI, Phoenix Technologies, and Microsoft.

https://arstechnica.com/security/2024/01/new-uefi-vulnerabilities-send-firmware-devs-across-an-entire-ecosystem-scrambling/

Malicious Chinese SDK In 1,200 iOS Apps With Billions Of Installs Causing ‘Major Privacy Concerns To Hundreds Of Millions Of Consumers’

Forbes

John Koetsier • August 24, 2020

A Chinese ad network named Mintegral is accused of spying on user activity and committing ad fraud in more than 1,200 apps with 300 million installs per month since July 2019. Mintegral is headquartered in Beijing, China, and is owned by another Chinese ad network, Mobvista, which has a head office in Guangzhou, China.

One of the apps, Helix Jump, has over 500 million total installs. Other popular apps that are impacted include Talking Tom, PicsArt, Subway Surfers and Gardenscapes.

All together, this likely impacts billions of total app installs on iPhone and iPad.

There’s no exact number on how many devices or iPhone users are impacted, but Snyk says this is a “major privacy concern to hundreds of millions of consumers.”

https://www.zdnet.com/article/ciscos-warning-critical-flaw-in-ios-routers-allows-complete-system-compromise/

Pre-installed malware

ars TECHNICA

NO FREE LUNCH —

US Government-funded Android phones come preinstalled with unremovable malware

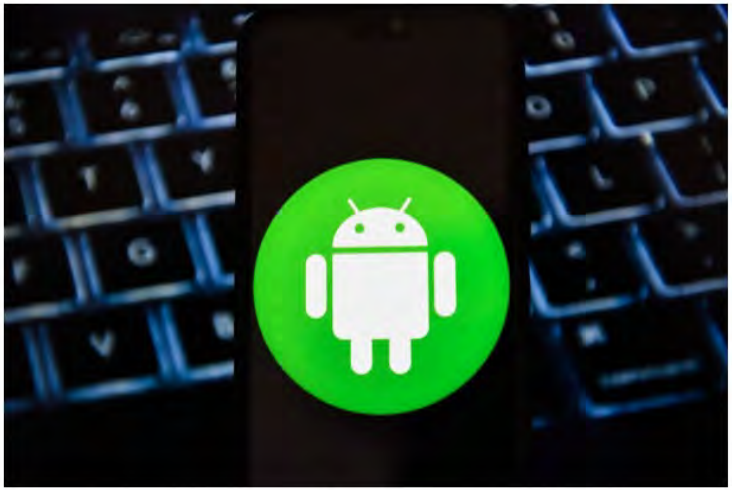
Phones were sold to low-income people under the FCC's Lifeline Assistance program.

DAN GOODIN - 1/9/2020, 4:26 PM

Android malware that comes preinstalled is a massive threat

The Android Security team's former tech lead, who's now a security researcher on Google's Project Zero, breaks down why.

Alfred Ng Aug. 8, 2019 2:30 p.m. PT



When malware comes preinstalled on Android devices, it's much harder to remove, Google's researchers said.

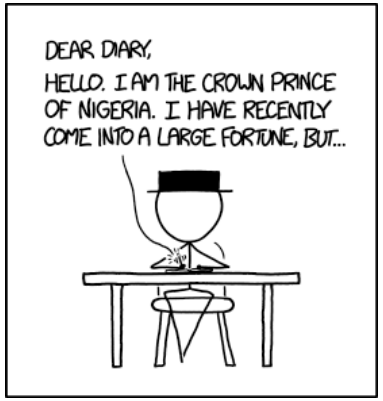
Omar Marques/SOPA Images/LightRocket via Getty Images

c|net

Don’t underestimate the human element

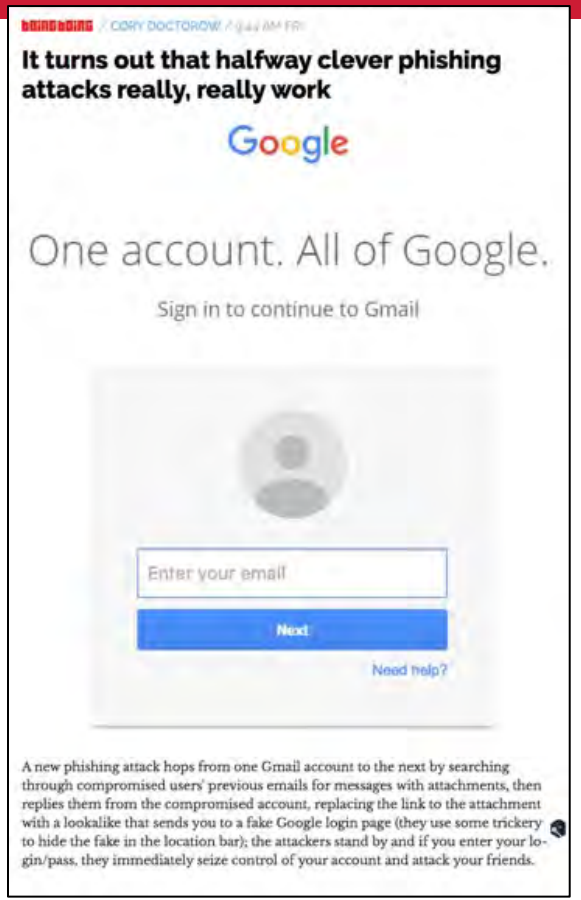
Humans are

- Bad at storing keys
- Poor at estimating risk
- Not accurate
- Careless
- Gullible



https://xkcd.com/1777/

Social engineering is the top threat



The End