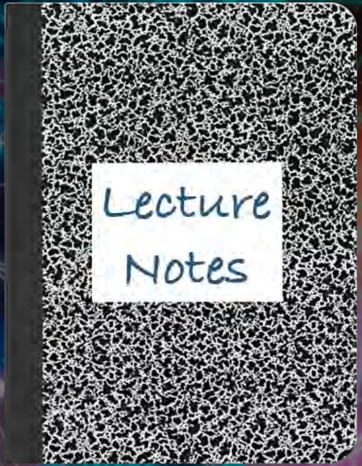
CS 419: Computer Security

Week 1: Part 3

Adversaries



Paul Krzyzanowski

Who are the adversaries?

- **Hackers**
  - Good or evil (or in between)
    - **Black hat hackers**: break into systems with malicious intent
    - **White hat hackers**: "ethical hackers" – discover vulnerabilities to help safeguard organizations
    - **Gray hat hackers**: in between – search for vulnerabilities without permission; may request payment
  - Test boundaries of the system – get to know the system better than the 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
- **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

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?

- **Hacktivists, Terrorists (freedom fighters)**
  - Motivated by geopolitics, religion, or a set of ethics
  - Examples:
    - **Anonymous Sudan** – targets anti-Muslim activities but may be Russian-backed
    - **Cyber Partisans** – Belarusian hacktivists against the Belarusian government
    - **DCLeaks** – claims to be Americans concerned with freedom of speech but at least some individuals were Russian
    - **Decocidio** – an autonomous hacking group part of Earth First, a radical environmental protest group
    - **Honker Union** – group in China mostly attacking U.S. websites
    - **Garnesia_Team**, **Moroccan Black Cyber Army** – pro-Palestinian attacks
    - **Ukrainian Cyber Alliance** – Ukrainian hackers fighting Russia
  - Usually more concerned with causing harm than getting specific information
  - Often (but not always) has low budgets & low skill levels
  - Some groups have grown more sophisticated
    - *IT Army of Ukraine* vs. Russia's *KillNet* group

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, Nation states**
  - 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 (not proven)
    - NSA planted backdoors into Cisco routers built for export that allow the NSA to intercept any communications through those routers.

Naming Schemes for APT Groups

Names usually come from organizations that identify the attacker

- There is no standard naming convention

1. APT Numbering

Coined by Mandiant (now part of FireEye)

- Sequential numbers in order of discovery
  - **APT1** – attributed to the 2nd Bureau of China's People's Liberation Army – Unit 6139
  - **APT29** – attributed to Russia's Foreign Intelligence Service

2. Animal Themes

Used by CrowdStrike

- **Panda**: Chinese APTs (Deep Panda, Gothic Panda, ...)
- **Bear**: Russian APTs (Cozy Bear, Fancy Bear, ...)
- **Kitten**: Iranian APTs (Charming Kitten)
- **Tiger**: Indian APTs (Patchwork Tiger)

Naming Schemes for APT Groups

3. Numeric Codes

Used by FireEye, Palo Alto Networks

- E.g., Group-3390, UNC2452
- Tracked until more details are confirmed about their origin

4. Threat Actor Names

Named after campaigns or characteristics

- Lazarus Group: North Korean group infamous for the Sony Pictures hack
- Equation Group: allegedly linked to the NSA

5. Microsoft Naming Scheme

Two-word combination of

Weather – identifies geography

Adjective or *noun*: identifies the group

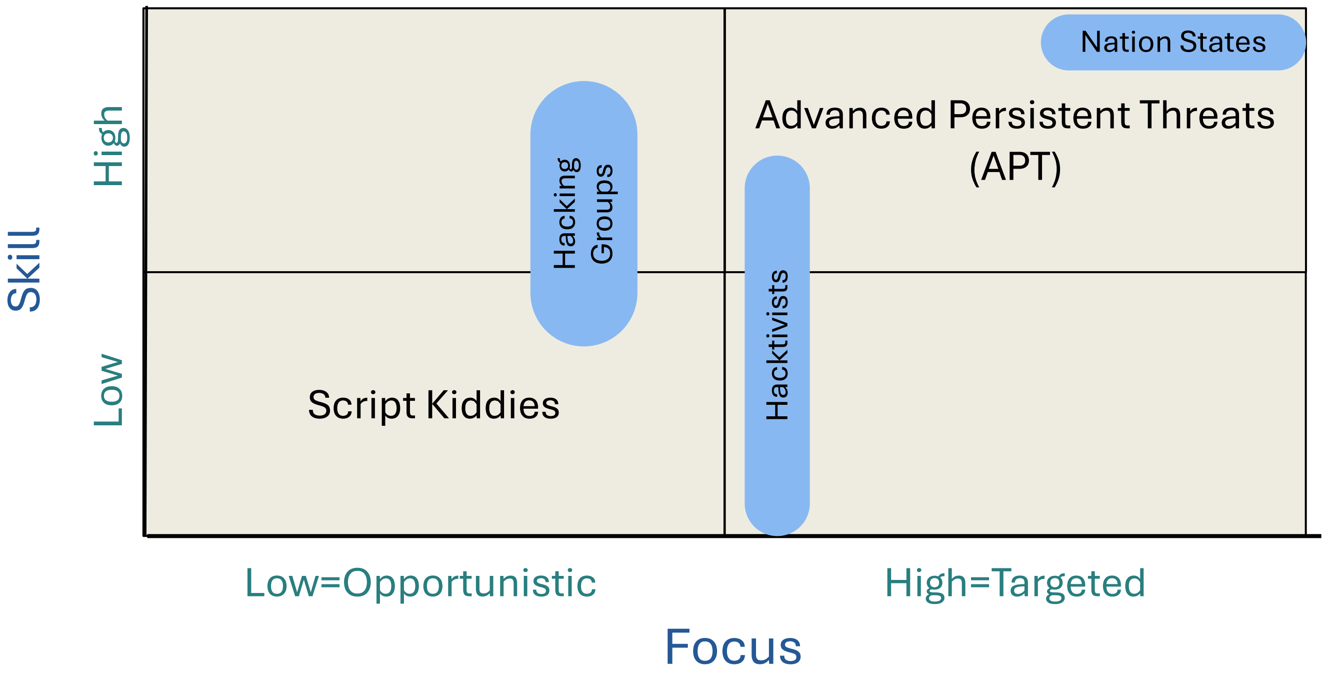
- Weather Terms
  - Typhoon: China
  - Cyclone: Iran
  - Blizzard: Russia
  - Sleet: North Korea
  - Sandstorm: Middle East
  - Tempest: Financially-motivated groups
  - Storm: Unconfirmed threat group
- E.g., Salt Typhoon, Midnight Blizzard

The different characteristics of attackers

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

Threat Matrix

Assess adversaries by skill vs. focus



Script Kiddies

- **Nov 2024: Script Kiddie 'Matrix' Builds Massive Botnet [link]**
  - Likely Russian Hacker Exploits IoT Vulnerabilities, Many Known for Years
  - Exploits IoT device vulnerabilities such as default credentials and outdated software.
  - Heavy reliance on external scripts and existing tools
- **July 2024: New FishXProxy Phishing Kit Making Phishing Accessible to Script Kiddies [link]**
  - A new phishing kit, FishXProxy, makes it alarmingly easy for cybercriminals to launch deceptive attacks.
- **July 2024: Botnets are being sold on the dark web for as little as $99 [link]**
  - More than 20 offers for botnets for hire or sale have been discovered on dark web forums and Telegram channels this year
- **Jan 2023: ChatGPT is enabling script kiddies to write functional malware [link]**
- **Nov 2019: Wannabe Fraudsters Can Buy Hacking Tools on Dark Web [link]**
  - Prices Start as Low as a Cup of Coffee

Launching a Ransomware Attack Against a 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.

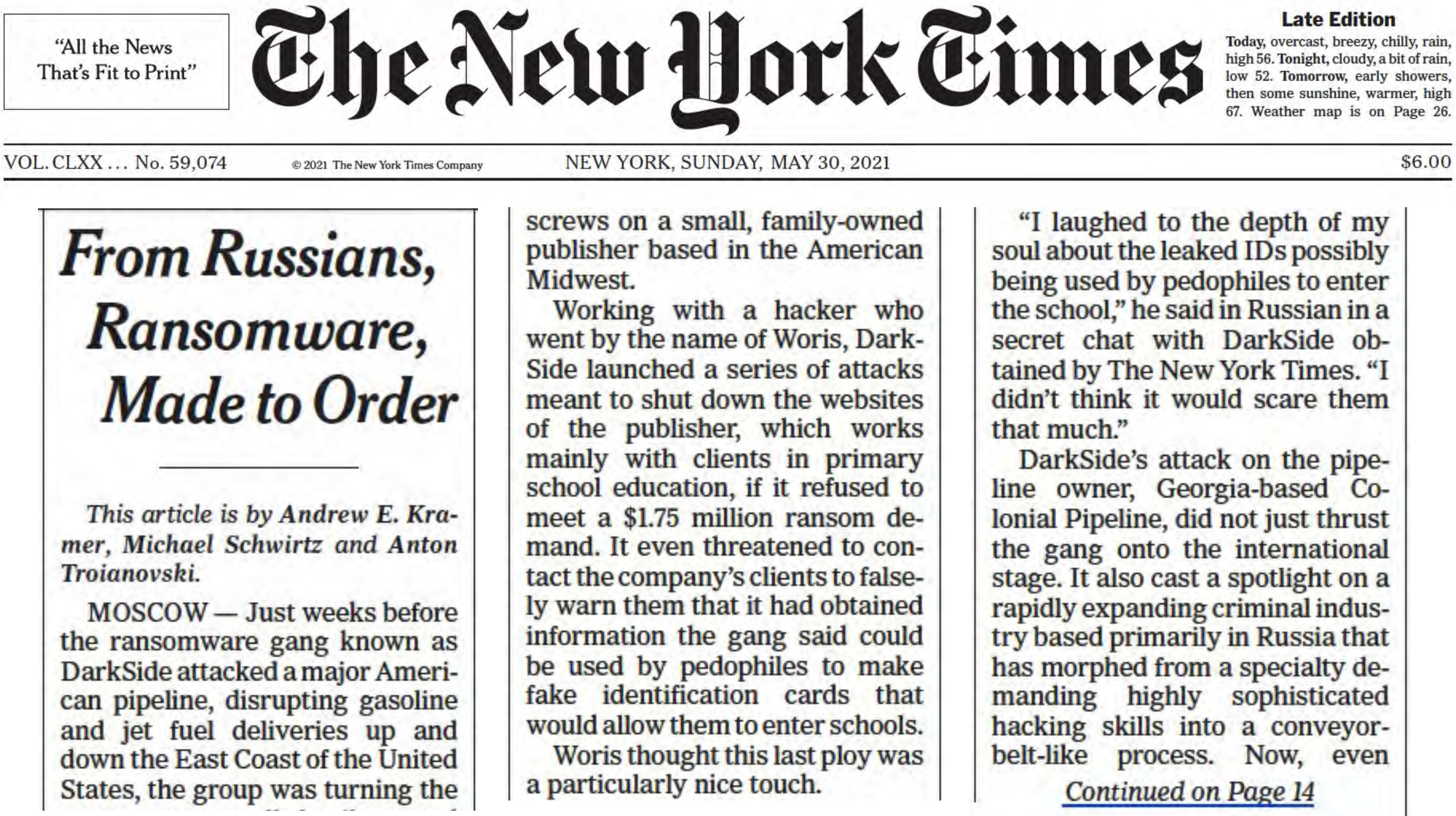
A U.S. military cyberwarfare officer who spoke to Newsweek on the condition of anonymity described a very simple process for doing a great deal of damage.

"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 © 2021 The New York Times Company 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

Cyber Warfare:
Nation State Attacks

2024 Highlights: State-Sponsored Espionage (1)

1. **Salt Typhoon Campaign (Year-long)**
   Chinese actors targeted telecoms globally, compromising surveillance systems and wiretap platforms

2. **Microsoft Email Breach (January)**
   Russian state-sponsored group Midnight Blizzard breached Microsoft's corporate emails, targeting leadership and legal teams for espionage.

3. **Pro-Palestinian Internet Archive Attack (October)**
   SN_BlackMeta launched a DDoS attack and stole user data for 33M from the Internet Archive

4. **Iran's Hack of Trump Campaign (August)**
   The breach was attributed to Iranian actors who exposed campaign documents

2024 Highlights: State-Sponsored Espionage (2)

1. **North Korean IT Worker Espionage (May–July)**
   North Korean agents infiltrated U.S. job markets, including an email security firm, to deploy malware and fund nuclear programs.

2. **Iran's Hack of Trump Campaign (August)**
   Breach attributed to Iranian actors, exposing campaign documents.

3. **Chinese Telecom Breaches (November)**
   U.S. telecoms compromised, leaking call records and surveillance information.

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

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 across 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**

Chinese hack of US telecoms compromised more firms than previously known, WSJ says

REUTERS®

Reuters • January 5, 2025

WASHINGTON, Jan 5 (Reuters) - A Chinese hack compromised even more U.S. telecoms than previously known, including Charter Communications, Consolidated Communications and Windstream, the Wall Street Journal reported late on Saturday, citing people familiar with the matter.

Hackers also exploited unpatched network devices from security vendor Fortinet and compromised large network routers from Cisco Systems, the newspaper reported.

In addition to deep intrusions into AT&T and Verizon (VZ.N, hackers pierced other networks belonging to Lumen Technologies and T-Mobile, according to the report.

China denied engaging in such actions and accused the United States of peddling disinformation.

https://www.reuters.com/business/media-telecom/chinese-hack-us-telecoms-compromised-more-firms-than-previously-known-wsj-says-2025-01-05/

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.

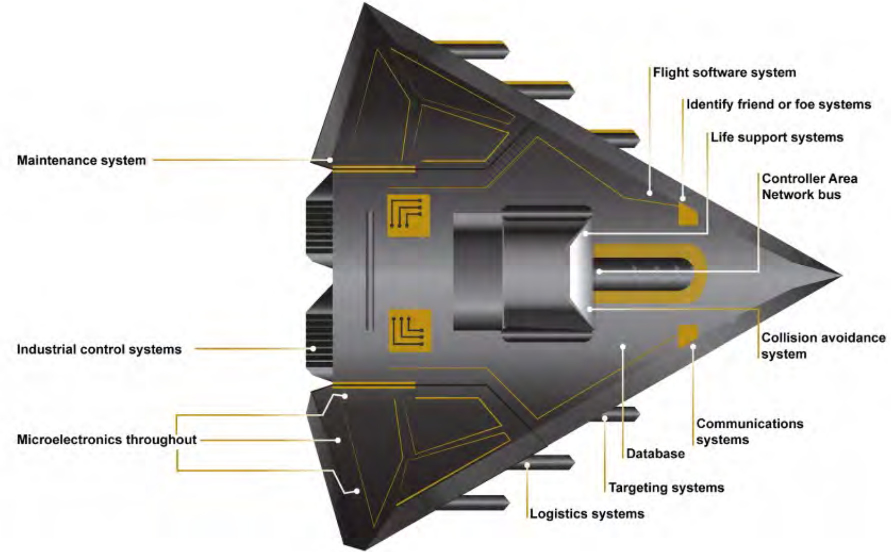
The new report is a summary of the IG's investigations into Pentagon cybersecurity over the previous year. It looked at 20 unclassified and four classified reports that detailed problems with cybersecurity and followed up to see if they'd been addressed. Previously, the IG had recommended the Pentagon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



Flight software system
Identify friend or foe systems
Life support systems
Maintenance system
Controller Area Network bus
Industrial control systems
Collision avoidance system
Communications systems
Microelectronics throughout
Database
Targeting systems
Logistics systems

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**

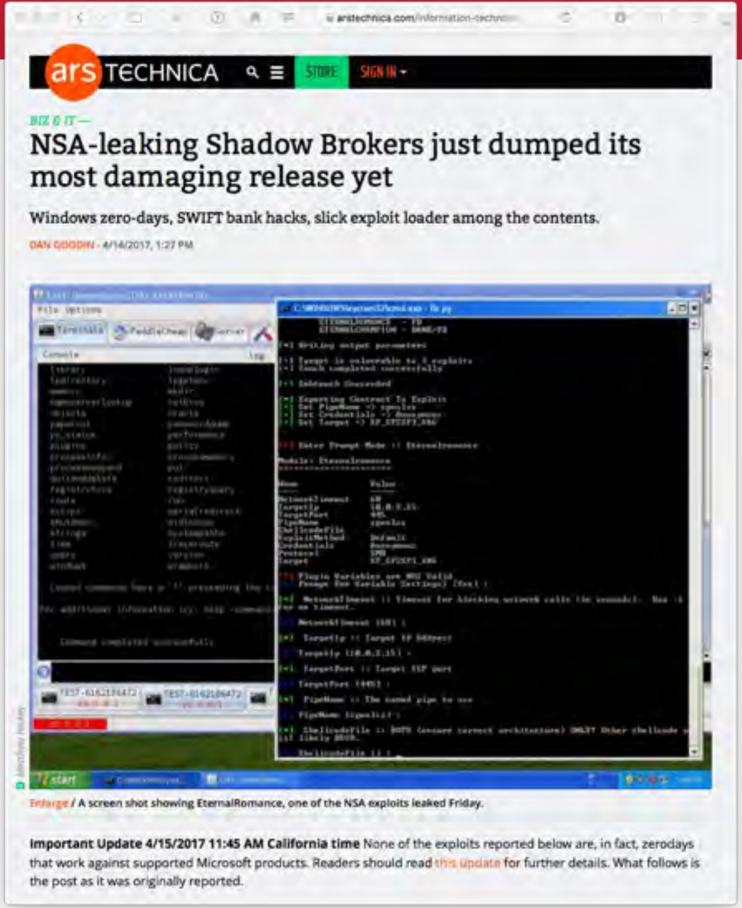
April 2017 – Theft from the NSA

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



BIZ & IT —

NSA-leaking Shadow Brokers just dumped its most damaging release yet

Windows zero-days, SWIFT bank hacks, slick exploit loader among the contents.

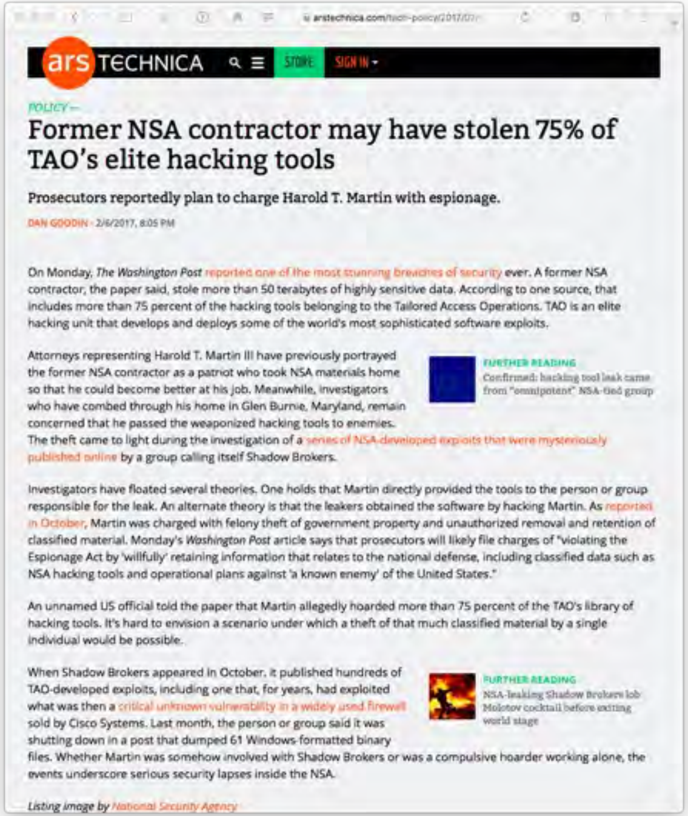
DAN GOODIN - 4/14/2017, 1:27 PM

Enlarge / A screen shot showing EternalRomance, one of the NSA exploits leaked Friday.

Important Update 4/15/2017 11:45 AM California time None of the exploits reported below are, in fact, zerodays that work against supported Microsoft products. Readers should read this update for further details. What follows is the post as it was originally reported.

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."***



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)**
  - Hacking, extortion (ransomware), scams (pyramid schemes, fake auctions, ...)
- **Extortion**
- **Scams**
  - Pay $$ and get little or nothing back: pyramid schemes, fake auctions
- **Destruction**

Attack Motives: Privacy violations

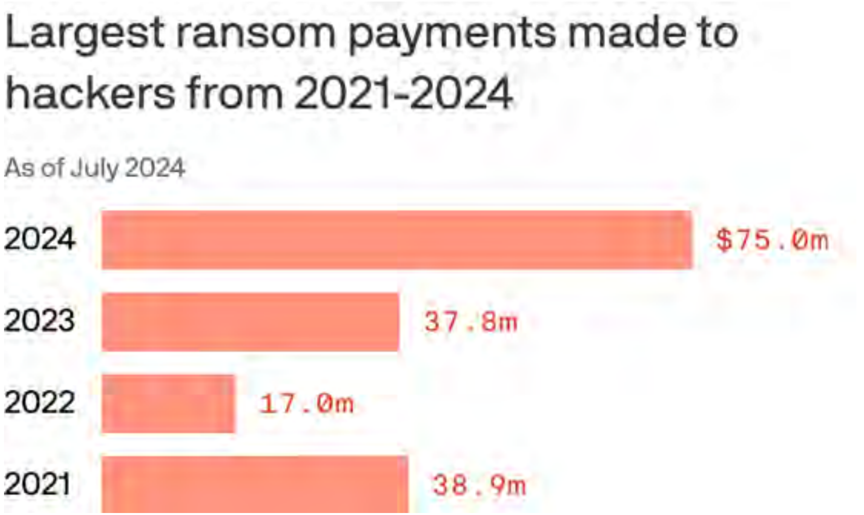
- **Intellectual property theft**
  - Challenge: sometimes we want to make data (e.g., software, music, movies, photos, books) accessible but keep control of its distribution
- **Identity theft**
- **Surveillance**
  - Databases
  - Installation of surveillance software
  - Traffic analysis
  - Large-scale surveillance
    - E.g., U.S. NSA's ECHELON, China Skynet

Profit

Ransomware can be highly profitable

Ransomware allows direct monetization of attacks

- **2023**
  - Median price paid to attackers: $200,000
  - Highest price: $37.8 million
- **2024**
  - Median price paid to attackers: $1,500,000
  - Highest price: $75 million



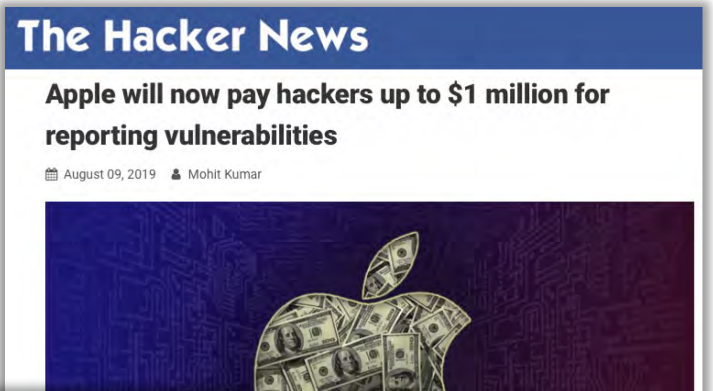
Data: Chainalysis; Note: 2024 record as of July; Chart: Axios Visuals

Some ransomware attacks

- **CDK Global (serving car dealerships) – June 2024 – crippled car sales – $25M**
- **Colonial Pipeline – May 2021 — Stopped fuel delivery – $4.4M**
- **Costa Rican govt – April 2022 – shut down multiple govt systems - $30M/day**
- **JBS Meats – May 2021 – Stopped meat delivery – $11M**
- **Kronos – December 2021 – workforce mgmt software affected numerous companies**
- **Maersk – June 2017 – shipping company suffered ~$300M in losses – 2 weeks to recover**
- **Acer – March 2021 – demanded $50M**
- **Brenntag – chemical distribution – $4.4M**
- **Kaseya – IT monitoring – 800-1500 businesses – demanded $70M**
- **Quanta – contract manufacturing (Apple) – demanded $50M**

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

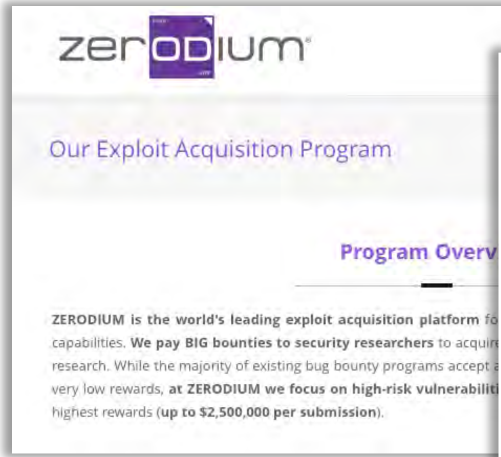


The Hacker News

Apple will now pay hackers up to $1 million for reporting vulnerabilities

August 09, 2019 Mohit Kumar

es of its bug bounty program by announcing a few major changes
Black Hat security conference yesterday.



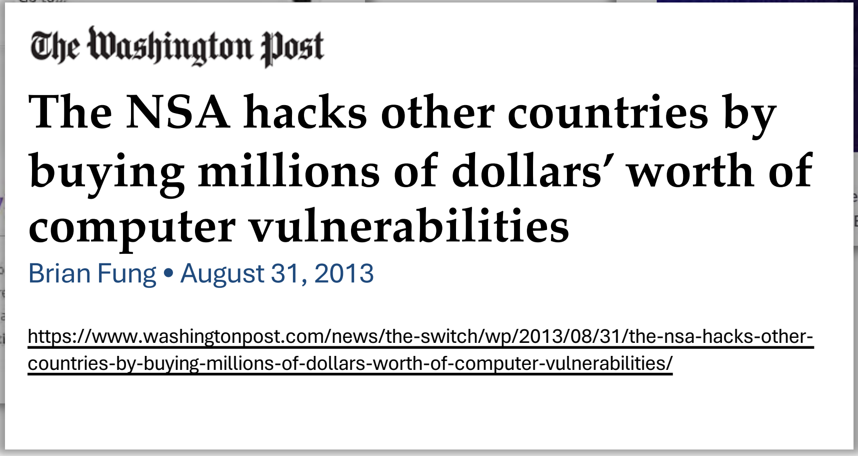
zerODIUM

Go to...

Our Exploit Acquisition Program

Program Overv

ZERODIUM is the world's leading exploit acquisition platform fo
capabilities. We pay BIG bounties to security researchers to acquire
research. While the majority of existing bug bounty programs accept a
very low rewards, at ZERODIUM we focus on high-risk vulnerabiliti
highest rewards (up to $2,500,000 per submission).



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/

Blockchain bridge Wormhole pays record $10m bug bounty reward

The Daily Swig
Cybersecurity news and views

Adam Bannister • May 23, 2022

An ethical hacker has earned a record $10 million bug bounty reward after discovering a critical security vulnerability in the Wormhole core bridge contract on Ethereum.

Wormhole is a decentralized, universal message-passing protocol that enables interoperability between blockchains such as Ethereum, Terra, and Binance Smart Chain (BSC).

Held to ransom

An attacker exploiting the vulnerability "could have held the entire protocol [to] ransom with the threat that the Ethereum Wormhole bridge would be bricked, and all the funds residing in that contract lost forever", according to a proof of concept (PoC) posted to GitHub by Immunefi.

The PoC also noted that "$736 million worth of assets [were] residing in the contract at the time of submission".

https://portswigger.net/daily-swig/blockchain-bridge-wormhole-pays-record-10m-bug-bounty-reward

Hackers get $886,250 for 49 zero-days at Pwn2Own Automotive 2025

BLEEPINGCOMPUTER

Sergiu Gatlan • January 24, 2025

The Pwn2Own Automotive 2025 hacking contest has ended with security researchers collecting $886,250 after exploiting 49 zero-days.

- The Synacktiv team used a single integer overflow to exploit the Sony IVI.
- The Synacktiv team used a single buffer overflow to exploit the Autel MaxiCharger.
- Thanh Do of Team Confused was able to confuse the Alpine iLX-507 with a single stack buffer overflow.
- The PHP Hooligans used a single OS command injection bug to exploit the Kenwood DMX958XR.
- Sina Kheirkhah of Summoning Team used a command injection bug on the Alpine iLX-507.
- Evan Grant used an OS command injection bug to exploit the Kenwood DMX958XR.

https://www.bleepingcomputer.com/news/security/hackers-get-886-250-for-49-zero-days-at-pwn2own-automotive-2025/

https://www.zerodayinitiative.com/blog/2025/1/23/pwn2own-automotive-2025-day-three-and-final-results

Paying for exploits – supply & demand

Price of zero-day exploits rises as companies harden products against hackers

TechCrunch

A startup is now offering millions of dollars for tools to hack iPhones, Android devices, WhatsApp, and iMessage

April 6, 2024

Tools that allow government hackers to break into iPhones and Android phones, popular software like the Chrome and Safari browsers, and chat apps like WhatsApp and iMessage, are now worth millions of dollars — and their price has multiplied in the last few years as these products get harder to hack.

On Monday, startup Crowdfense published its updated price list for these hacking tools, which are commonly known as “zero-days” because they rely on unpatched vulnerabilities in software that are unknown to the makers of that software.

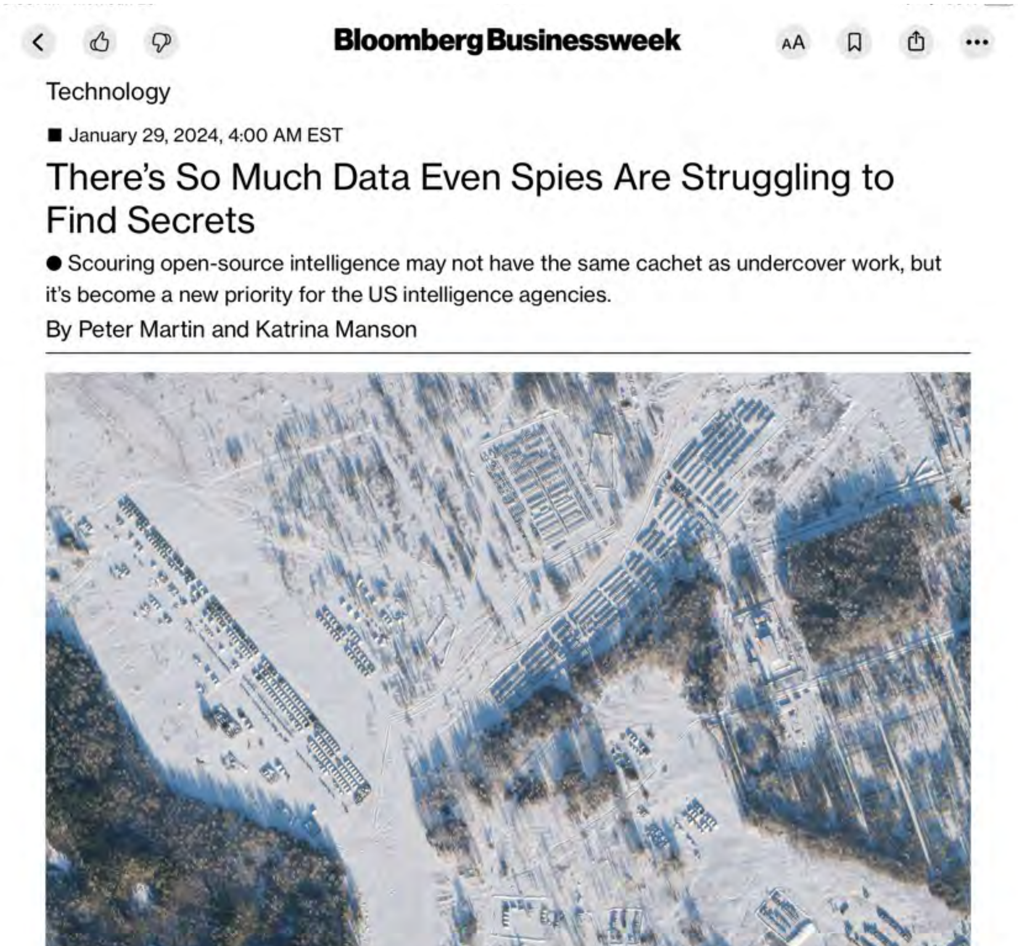
Companies like Crowdfense and one of its competitors, Zerodium, claim to acquire these zero-days with the goal of reselling them to other organizations, usually government agencies or government contractors, which claim they need the hacking tools to track or spy on criminals.

https://techcrunch.com/2024/04/06/price-of-zero-day-exploits-rises-as-companies-harden-products-against-hackers/

Attack Motives: Privacy violations

Surveillance

- Databases
- Installation of surveillance software
- Traffic analysis
- Large-scale surveillance
  - E.g., ECHELON, Skynet



Bloomberg Businessweek

Technology

■ January 29, 2024, 4:00 AM EST

There's So Much Data Even Spies Are Struggling to Find Secrets

● Scouring open-source intelligence may not have the same cachet as undercover work, but it's become a new priority for the US intelligence agencies.

By Peter Martin and Katrina Manson

Other motives

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

HACKERS BRIEFLY TOOK DOWN THE WEBSITE OF THE CIA YESTERDAY...
WHAT PEOPLE HEAR:
SOMEONE HACKED INTO THE COMPUTERS OF THE CIA!!
WHAT COMPUTER EXPERTS HEAR:
SOMEONE TORE DOWN A POSTER HUNG UP BY THE CIA!!

The End