T-401-ICYB
Introduction to Cyber Security

Stephan Schiffel

24.11.2025

Outline

1. Course Logistics
2. The problem: Attack Surface
3. History of Attacks
4. Cyber Defence
5. Computer Security Evolution
6. Up Next ...

Course Logistics

Course Contents

- What is Cyber Security
- Linux + Windows command line tools
- Operating Systems Basics (Access Control)
- Networking Basics
- Virtualization
- Web Security / Attacks
- Common Tools for Security Testing
- Principles of Defense
- Guest Lectures: Phishing, Information Warfare, Binary Exploitation

Course Requirements - Background

- Basic Programming: Python, Shell Scripts
- Computer Architecture
- Report Writing

Course Material

- Specific reading will be provided with the lectures
- You should expect to spend several hours a week reading
- Group assignment (CySec Knowledge Base) should be used to organize material and notes

Good Use of AI

- **Idea Generation & Brainstorming**
  - How can I do X?
  - Stimulate creative thinking for projects/essays.
- **Clarification & Conceptual Understanding**
  - Get concepts explained in simpler terms or with examples.
  - Deepen comprehension by exploring different perspectives.
- **Resource Discovery & Study Planning**
  - Locate relevant sources, structure study schedules.
- **Writing Support & Refinement**
  - Check grammar, suggest phrasing, expand vocabulary.
  - *Crucially: The content must be your original thought.*
- **Summarization & Information Synthesis**
  - Grasp core concepts from long texts quickly.
  - Identify key arguments for efficient review.

Use AI to augment your abilities, not to replace them.

AI Tools for Learning: Pitfalls to Avoid

- **Academic Dishonesty (Plagiarism)**
  - Submitting AI-generated work as your own without proper attribution.
  - Violates integrity, **prevents genuine learning**.
- **Over-Reliance & Skipping Critical Thinking**
  - Getting direct answers without attempting to solve yourself.
  - Undermines problem-solving skills, reduces critical analysis.
- **Lack of Verification & Fact-Checking**
  - Uncritically accepting AI output; AI can ”hallucinate” incorrect info.
  - Leads to misinformation, demonstrates lack of scholarly rigor.
- **Substituting Personal Effort & Engagement**
  - Avoiding reading or formulating your own thoughts/responses.
  - **Limits intellectual growth, weakens understanding.**
- **Privacy Risks**
  - Sharing confidential, sensitive, or personal information with AI tools.

Don’t let AI replace your learning process, critical thinking, or academic integrity.

Equipment

- Laptop or similar capable of running hosted VM.
- Some labs will run on your laptop, some on VMs
- Linux, OSX or Windows ok
- Backup your laptop! (in case something goes wrong)

Program

- 9:00 - 12:00 :: Lecture, Reading, Note Taking, Quiz
- 12:40 - 16:00 :: Lab assignment
- Friday 12.12. :: Exam

Assessment

- 30% Quizzes (to be done individually)
- 30% Lab Assignments (groups of 3-4 students)
- 10% CySec Knowledge Base (groups of up to 12 students)
- 30% Final Exam (individually)

Communication

- Piazza and Discord
- Piazza (private posts) for individual issues and grade issues during the course
- Email only if really necessary
- All submissions will be made on Canvas

Hazard Warning

- We will be playing with fire.
- Do not try techniques covered here on computers you do not control or have permission to test.
- Do not download random executables from the Internet.
- Obtain permission of instructor if you are in any doubt whatsoever.
- Always get permissions in writing.
- Be careful with any code or instructions you find online.

The problem: Attack Surface

The Attack Surface

”The sum of all potential vulnerabilities in a system where an attacker could try to subvert the intended purpose of the system and organisation or person who is using it.”

The Attack Surface (2)

- Email - can contain viruses, malware, links to bad sites
- All network points of access (Wired, Wifi, Bluetooth, ...)
- USB, CDROM, Hard drives, (Floppy drives)
- Downloaded viruses and malware
  - May be embedded in legitimate documents or software
  - Free games, personality tests, ...
- SMS messages
- Software Distributions, External Software, Bios, Chips, ...
- etc.

i.e. any form of input or control over software or machine

What are the Real Risks?

Assume:

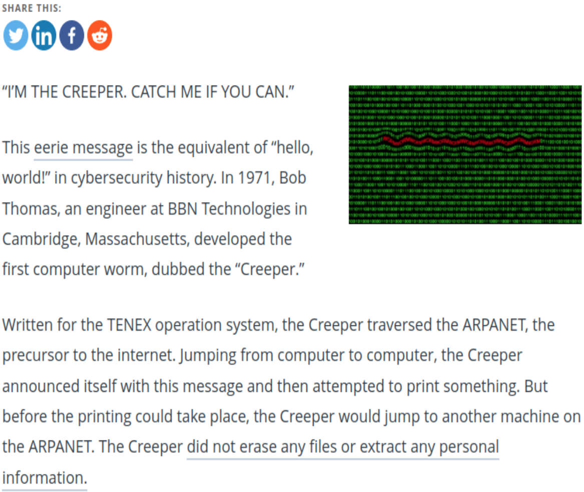
- Secure Machine: All ports closed
- Local firewall enabled
- All software updates applied

Risks:

- Inadvertant Virus introduction (email, usb, evil web site, trojan software)
- Unpatched (not up to date) software versions
- Zero day exploit in OS
- Zero day exploit in Network Application
- Web Browser Malware
- Hardware backdoor (Intel Management System)
- IT security failure

History of Attacks

Arpanet: Creeper (PDP11, Tenex OS)



SHARE THIS:

"I'M THE CREEPER. CATCH ME IF YOU CAN."

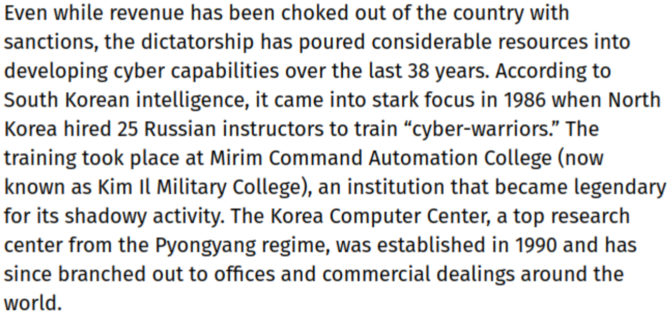
This eerie message is the equivalent of "hello, world!" in cybersecurity history. In 1971, Bob Thomas, an engineer at BBN Technologies in Cambridge, Massachusetts, developed the first computer worm, dubbed the "Creeper."

Written for the TENEX operation system, the Creeper traversed the ARPANET, the precursor to the internet. Jumping from computer to computer, the Creeper announced itself with this message and then attempted to print something. But before the printing could take place, the Creeper would jump to another machine on the ARPANET. The Creeper did not erase any files or extract any personal information.

1971

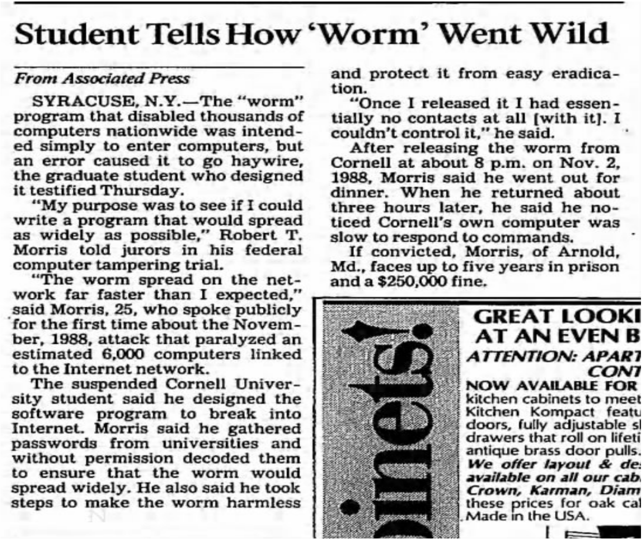
North Korea trains first ”cyber-warriors”

1986



Even while revenue has been choked out of the country with sanctions, the dictatorship has poured considerable resources into developing cyber capabilities over the last 38 years. According to South Korean intelligence, it came into stark focus in 1986 when North Korea hired 25 Russian instructors to train “cyber-warriors.” The training took place at Mirim Command Automation College (now known as Kim Il Military College), an institution that became legendary for its shadowy activity. The Korea Computer Center, a top research center from the Pyongyang regime, was established in 1990 and has since branched out to offices and commercial dealings around the world.

Morris Worm brings down 6,000+ Internet computers



Student Tells How 'Worm' Went Wild

From Associated Press

SYRACUSE, N.Y.—The "worm" program that disabled thousands of computers nationwide was intended simply to enter computers, but an error caused it to go haywire, the graduate student who designed it testified Thursday.

"My purpose was to see if I could write a program that would spread as widely as possible," Robert T. Morris told jurors in his federal computer tampering trial.

"The worm spread on the network far faster than I expected," said Morris, 25, who spoke publicly for the first time about the November, 1988, attack that paralyzed an estimated 6,000 computers linked to the Internet network.

The suspended Cornell University student said he designed the software program to break into Internet. Morris said he gathered passwords from universities and without permission decoded them to ensure that the worm would spread widely. He also said he took steps to make the worm harmless and protect it from easy eradication.

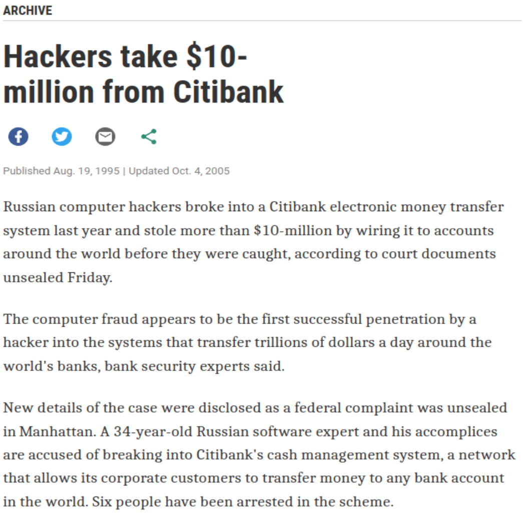
"Once I released it I had essentially no contacts at all [with it]. I couldn't control it," he said.

After releasing the worm from Cornell at about 8 p.m. on Nov. 2, 1988, Morris said he went out for dinner. When he returned about three hours later, he said he noticed Cornell's own computer was slow to respond to commands.

If convicted, Morris, of Arnold, Md., faces up to five years in prison and a $250,000 fine.

1988

$10 million Citibank attack



ARCHIVE

Hackers take $10-million from Citibank

Published Aug. 19, 1995 | Updated Oct. 4, 2005

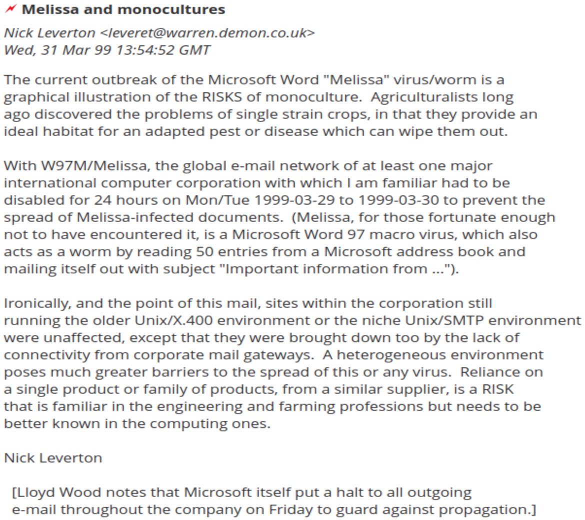
Russian computer hackers broke into a Citibank electronic money transfer system last year and stole more than $10-million by wiring it to accounts around the world before they were caught, according to court documents unsealed Friday.

The computer fraud appears to be the first successful penetration by a hacker into the systems that transfer trillions of dollars a day around the world's banks, bank security experts said.

New details of the case were disclosed as a federal complaint was unsealed in Manhattan. A 34-year-old Russian software expert and his accomplices are accused of breaking into Citibank's cash management system, a network that allows its corporate customers to transfer money to any bank account in the world. Six people have been arrested in the scheme.

1994

Windows 98: Melissa Email Worm brings down global email



Melissa and monocultures

Nick Leverton <leveret@warren.demon.co.uk>
Wed, 31 Mar 99 13:54:52 GMT

The current outbreak of the Microsoft Word "Melissa" virus/worm is a graphical illustration of the RISKS of monoculture. Agriculturalists long ago discovered the problems of single strain crops, in that they provide an ideal habitat for an adapted pest or disease which can wipe them out.

With W97M/Melissa, the global e-mail network of at least one major international computer corporation with which I am familiar had to be disabled for 24 hours on Mon/Tue 1999-03-29 to 1999-03-30 to prevent the spread of Melissa-infected documents. (Melissa, for those fortunate enough not to have encountered it, is a Microsoft Word 97 macro virus, which also acts as a worm by reading 50 entries from a Microsoft address book and mailing itself out with subject "Important information from ...").

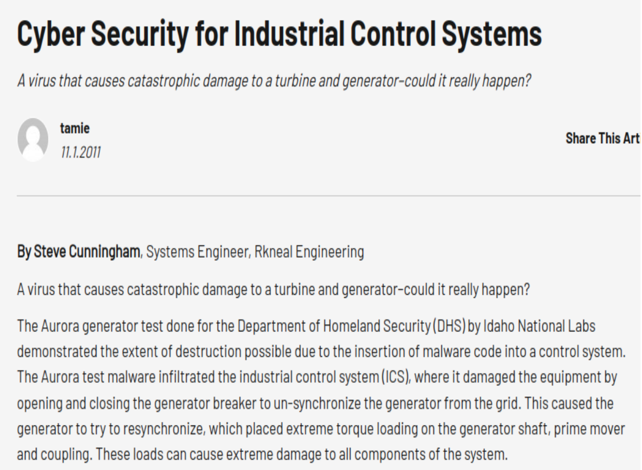
Ironically, and the point of this mail, sites within the corporation still running the older Unix/X.400 environment or the niche Unix/SMTP environment were unaffected, except that they were brought down too by the lack of connectivity from corporate mail gateways. A heterogeneous environment poses much greater barriers to the spread of this or any virus. Reliance on a single product or family of products, from a similar supplier, is a RISK that is familiar in the engineering and farming professions but needs to be better known in the computing ones.

Nick Leverton

[Lloyd Wood notes that Microsoft itself put a halt to all outgoing e-mail throughout the company on Friday to guard against propagation.]

1999

Aurora Generator Test: 30 lines of code destroys Power Generator



Cyber Security for Industrial Control Systems

A virus that causes catastrophic damage to a turbine and generator-could it really happen?

tamie
11.1.2011

Share This Art

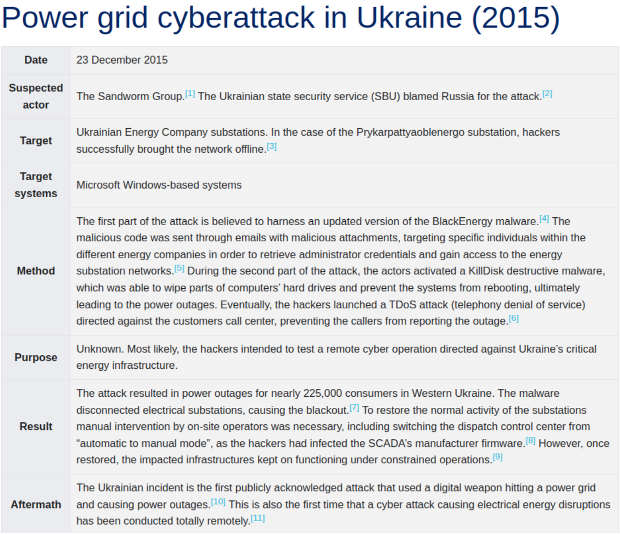
By Steve Cunningham, Systems Engineer, Rkneal Engineering

A virus that causes catastrophic damage to a turbine and generator-could it really happen?

The Aurora generator test done for the Department of Homeland Security (DHS) by Idaho National Labs demonstrated the extent of destruction possible due to the insertion of malware code into a control system. The Aurora test malware infiltrated the industrial control system (ICS), where it damaged the equipment by opening and closing the generator breaker to un-synchronize the generator from the grid. This caused the generator to try to resynchronize, which placed extreme torque loading on the generator shaft, prime mover and coupling. These loads can cause extreme damage to all components of the system.

2007

Ukrainian Power Grid Shutdown for 1-6 hours (23rd December 2015)



Power grid cyberattack in Ukraine (2015)

Date	23 December 2015
Suspected actor	The Sandworm Group.[1] The Ukrainian state security service (SBU) blamed Russia for the attack.[2]
Target	Ukrainian Energy Company substations. In the case of the Prykarpattyaoblenergo substation, hackers successfully brought the network offline.[3]
Target systems	Microsoft Windows-based systems
Method	The first part of the attack is believed to harness an updated version of the BlackEnergy malware.[4] The malicious code was sent through emails with malicious attachments, targeting specific individuals within the different energy companies in order to retrieve administrator credentials and gain access to the energy substation networks.[5] During the second part of the attack, the actors activated a KillDisk destructive malware, which was able to wipe parts of computers' hard drives and prevent the systems from rebooting, ultimately leading to the power outages. Eventually, the hackers launched a TDoS attack (telephony denial of service) directed against the customers call center, preventing the callers from reporting the outage.[6]
Purpose	Unknown. Most likely, the hackers intended to test a remote cyber operation directed against Ukraine's critical energy infrastructure.
Result	The attack resulted in power outages for nearly 225,000 consumers in Western Ukraine. The malware disconnected electrical substations, causing the blackout.[7] To restore the normal activity of the substations manual intervention by on-site operators was necessary, including switching the dispatch control center from "automatic to manual mode", as the hackers had infected the SCADA's manufacturer firmware.[8] However, once restored, the impacted infrastructures kept on functioning under constrained operations.[9]
Aftermath	The Ukrainian incident is the first publicly acknowledged attack that used a digital weapon hitting a power grid and causing power outages.[10] This is also the first time that a cyber attack causing electrical energy disruptions has been conducted totally remotely.[11]

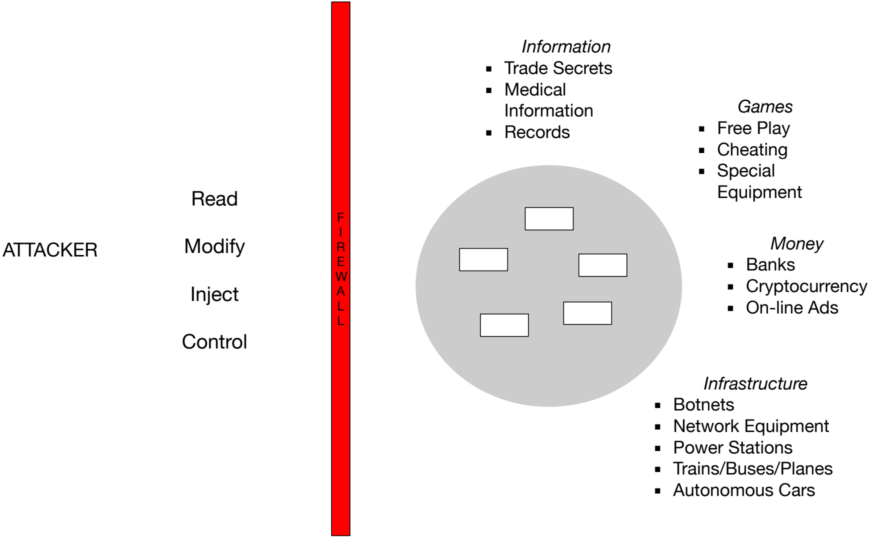
2015

Cyber Defence

What is Cyber Defence?

”Acting in anticipation to oppose an attack through cyber and cognitive domains.”

High Level View of Computer System Security



ATTACKER

Read

Modify

Inject

Control

FIREWALL

Information

- Trade Secrets
- Medical Information
- Records

Games

- Free Play
- Cheating
- Special Equipment

Money

- Banks
- Cryptocurrency
- On-line Ads

Infrastructure

- Botnets
- Network Equipment
- Power Stations
- Trains/Buses/Planes
- Autonomous Cars

Computer security involves ...

- Preventing and detecting unwanted access, use of computers, theft of data.
- Preventing and detecting unauthorized modification
- Preventing and detecting unauthorized injection of data, computers etc.

Job as Computer Professionals is to develop and maintain reliable computer systems. In the same way we expect Civil Engineers to build bridges that don't fall down, Civil Engineers -and everybody else - expects us to build to computer systems that can be relied on.

Categories of Computer Security Threat

- Unauthorized access
- Unauthorised modification
- Unauthorised disclosure
- Denial of Authorized Access
- Forgery
- Repudiation - where the integrity of an asset can be disputed
- Spoofing - masquerading as a legitimate entity

Still Missing:

- Information Warfare?
- Bribery/Blackmail?
- Deliberate Incompetance?
- Inducing system overload?

Computer Gaming "Security" Issues

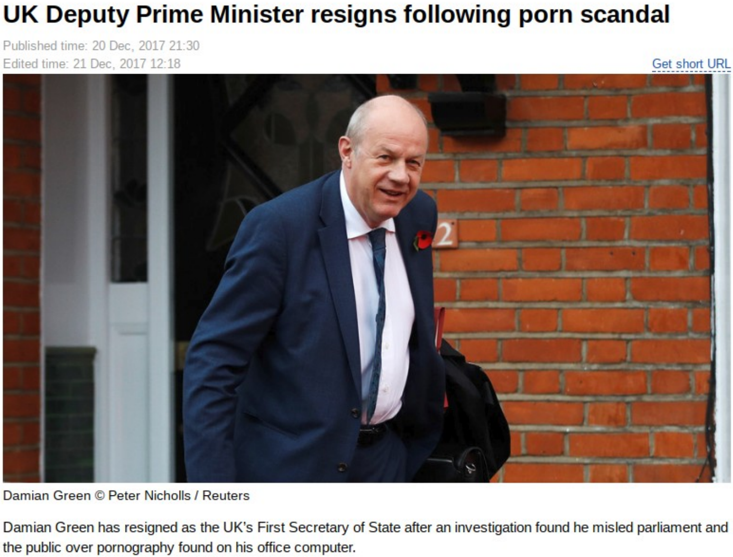
- Multiple Accounts
- Access to Game Database (Items)
- Disconnecting
- Farming
- Scripting
- 3rd Party Software (Poker Assistants, Aim Correction)
- etc.

~~None of which is illegal...~~

Video gamers who cheat online face up to 5 years in prison (S. Korea, 2022)

Other forms of Attack

- Denial of Service - Interrupt operations of company
- Modify information - Schools, Medical
- Physical Destruction - Stuxnet
- Infrastructure Attack - eg. Power station control points
- Ransomware - encrypt the hard drive
- Masquerade as victim - credit card fraud, dark net activities
- Add files - poison web cache
- Corporate Espionage
- Information Warfare



UK Deputy Prime Minister resigns following porn scandal

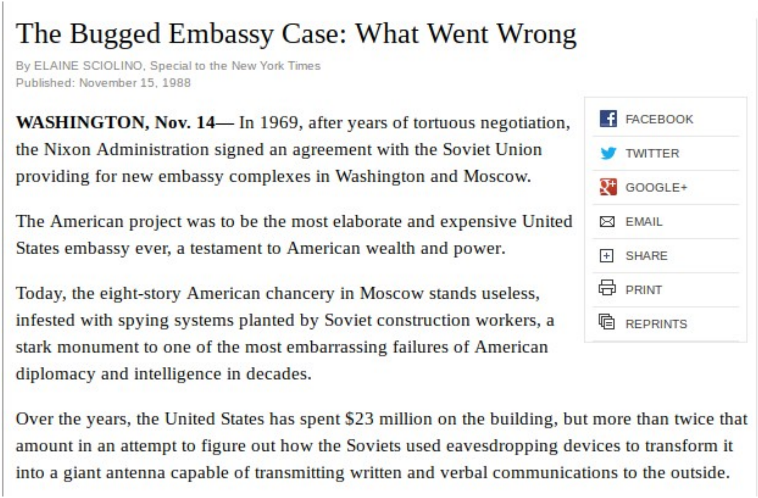
Published time: 20 Dec, 2017 21:30
Edited time: 21 Dec, 2017 12:18

Get short URL

Damian Green © Peter Nicholls / Reuters

Damian Green has resigned as the UK's First Secretary of State after an investigation found he misled parliament and the public over pornography found on his office computer.

If you want to subvert the democratic processes of another country, this is arguably easier than ...



The Bugged Embassy Case: What Went Wrong

By ELAINE SCIOLINO, Special to the New York Times
Published: November 15, 1988

WASHINGTON, Nov. 14— In 1969, after years of tortuous negotiation, the Nixon Administration signed an agreement with the Soviet Union providing for new embassy complexes in Washington and Moscow.

The American project was to be the most elaborate and expensive United States embassy ever, a testament to American wealth and power.

Today, the eight-story American chancery in Moscow stands useless, infested with spying systems planted by Soviet construction workers, a stark monument to one of the most embarrassing failures of American diplomacy and intelligence in decades.

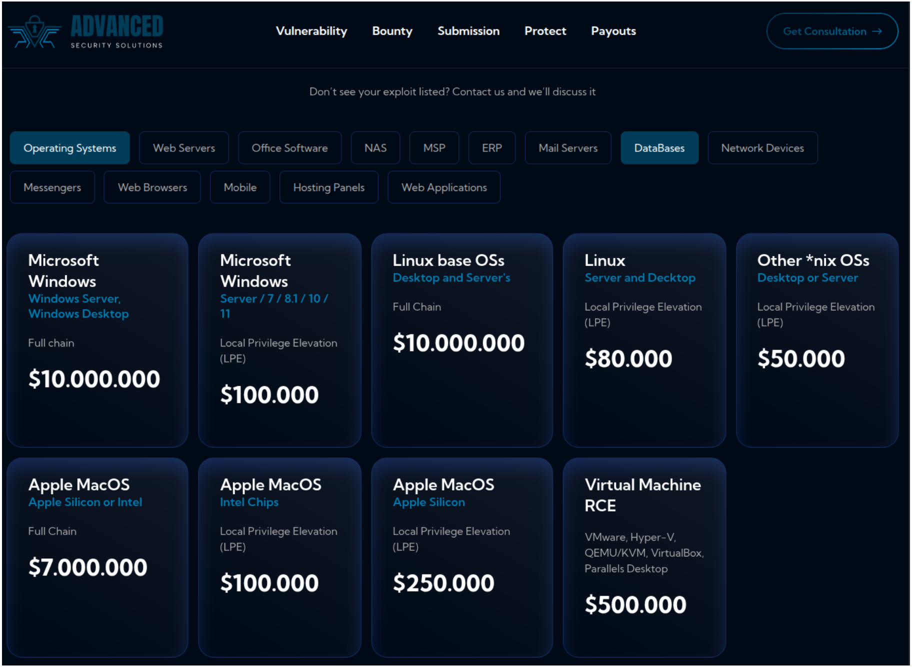
Over the years, the United States has spent $23 million on the building, but more than twice that amount in an attempt to figure out how the Soviets used eavesdropping devices to transform it into a giant antenna capable of transmitting written and verbal communications to the outside.

Source: `http://www.nytimes.com/1988/11/15/world/the-bugged-embassy-case-what-went-wrong.html`

Computer Security Evolution

Computer Security Evolution

- Prevent Attacks (programming and design quality)
- Testing!
- Manufacturers: Offer small sums of money to report bugs (Bug Bounties)
- Nation States: Offer large sums of money to buy attacks for future use (Zero-day bugs)
- And the consequence was...
- ... market based pricing providing a guide to relative security



Don't see your exploit listed? Contact us and we'll discuss it

Microsoft Windows
Windows Server, Windows Desktop
Full chain
$10.000.000

Microsoft Windows
Server / 7 / 8.1 / 10 / 11
Local Privilege Elevation (LPE)
$100.000

Linux base OSs
Desktop and Server's
Full Chain
$10.000.000

Linux
Server and Decktop
Local Privilege Elevation (LPE)
$80.000

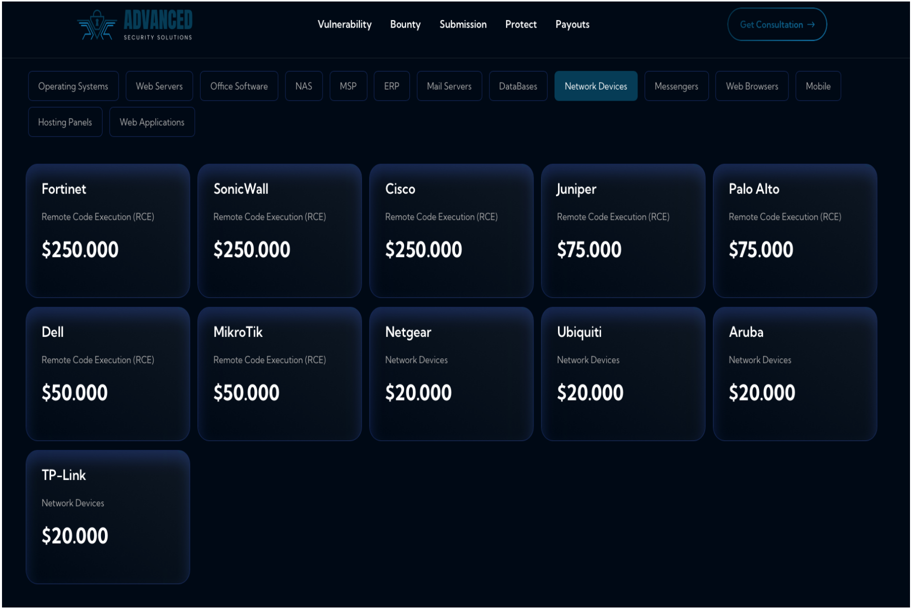
Other *nix OSs
Desktop or Server
Local Privilege Elevation (LPE)
$50.000

Apple MacOS
Apple Silicon or Intel
Full Chain
$7.000.000

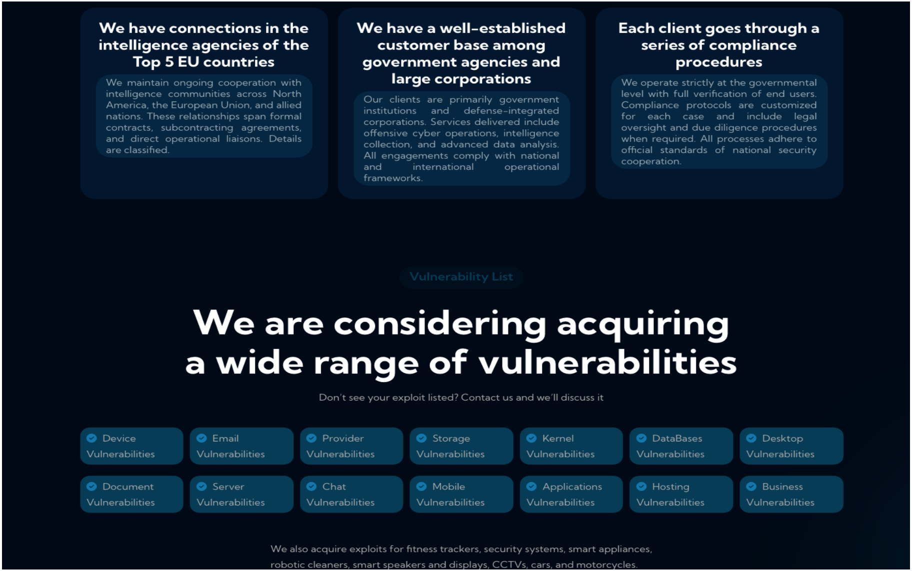
Apple MacOS
Intel Chips
Local Privilege Elevation (LPE)
$100.000

Apple MacOS
Apple Silicon
Local Privilege Elevation (LPE)
$250.000

Virtual Machine RCE
VMware, Hyper-V, QEMU/KVM, VirtualBox, Parallels Desktop
$500.000



Fortinet	Remote Code Execution (RCE)	$250.000
SonicWall	Remote Code Execution (RCE)	$250.000
Cisco	Remote Code Execution (RCE)	$250.000
Juniper	Remote Code Execution (RCE)	$75.000
Palo Alto	Remote Code Execution (RCE)	$75.000
Dell	Remote Code Execution (RCE)	$50.000
MikroTik	Remote Code Execution (RCE)	$50.000
Netgear	Network Devices	$20.000
Ubiquiti	Network Devices	$20.000
Aruba	Network Devices	$20.000
TP-Link	Network Devices	$20.000



We have connections in the intelligence agencies of the Top 5 EU countries

We maintain ongoing cooperation with intelligence communities across North America, the European Union, and allied nations. These relationships span formal contracts, subcontracting agreements, and direct operational liaisons. Details are classified.

We have a well-established customer base among government agencies and large corporations

Our clients are primarily government institutions and defense-integrated corporations. Services delivered include offensive cyber operations, intelligence collection, and advanced data analysis. All engagements comply with national and international operational frameworks.

Each client goes through a series of compliance procedures

We operate strictly at the governmental level with full verification of end users. Compliance protocols are customized for each case and include legal oversight and due diligence procedures when required. All processes adhere to official standards of national security cooperation.

Vulnerability List

We are considering acquiring a wide range of vulnerabilities

Don't see your exploit listed? Contact us and we'll discuss it

- ✓ Device Vulnerabilities
- ✓ Email Vulnerabilities
- ✓ Provider Vulnerabilities
- ✓ Storage Vulnerabilities
- ✓ Kernel Vulnerabilities
- ✓ DataBases Vulnerabilities
- ✓ Desktop Vulnerabilities
- ✓ Document Vulnerabilities
- ✓ Server Vulnerabilities
- ✓ Chat Vulnerabilities
- ✓ Mobile Vulnerabilities
- ✓ Applications Vulnerabilities
- ✓ Hosting Vulnerabilities
- ✓ Business Vulnerabilities

We also acquire exploits for fitness trackers, security systems, smart appliances, robotic cleaners, smart speakers and displays, CCTVs, cars, and motorcycles.

Up Next ...

Further Reading

Look into the following computer viruses and attacks and find out 1. how the viruses/attacks worked, 2. which impact they had and 3. which weakness(es) they used

- Creeper (1971)
- Morris Worm (1988)
- Vladimir Levin stealing 10 million USD from Citibank in 1994
- Melissa Email Worm (1999)
- Operation Olympic Games (2009)
- Ukrainian Power Grid Shutdown (23rd December 2015)
- WannaCry Ransomware Attack (2017)

Lab 1

- Check the Security of your own system!
- Useful resources:
  - `https://nvd.nist.gov` (US) National Vulnerability Database
  - `https://www.cve.org`, `https://www.cvedetails.com`
    Maintains searchable database of CVE's (Common Vulnerabilities and Exposures)
    Sponsored by US Dept. of Homeland Security
    Restricted to publicised vulnerabilities
  - `https://www.exploit-db.com`
    Public open source database of vulnerabilities

Unix Fortune Cookie

If builders built buildings the way programmers wrote programs, then the first woodpecker that came along would destroy civilization.
Gerald Weinberg (circa 1980)

"In the 20th century, war is with bullets over oil. But in the 21st century, war will be fought as information warfare"

Kim Jong-il Directive to KPA General Staff (1995)