CYLANCE

Operation Cleaver – A precursor to control system attacks

Jon Miller

Agenda

Introduction

What is Cylance

What is the Problem

Operation Cleaver

Vulnerabilities

Augmenting

Introduction

Jon Miller | Vice President of Strategy

Internet Security Systems
(5 years)

- X-Force Penetration Testing
- Special Advisor to CTO

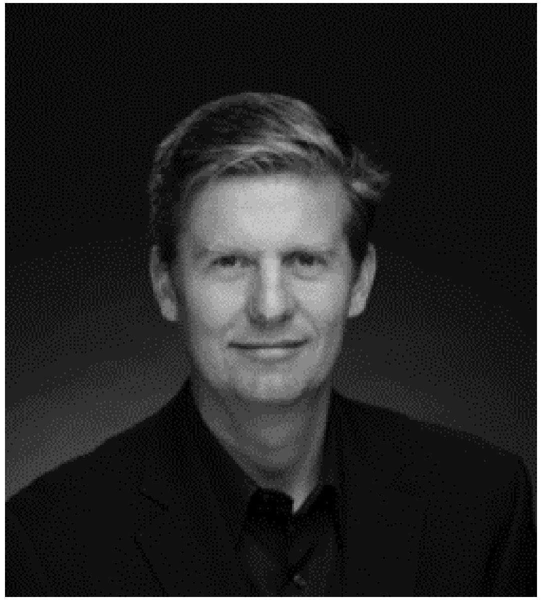
Accuvant Labs
(7 years)

- Penetration Testing
- Reverse Engineering
- Weaponized 0day Sales

Cylance
(2 Years)

- Internal Security
- Product Testing/Efficacy
- SPEAR Research Team
- Customer Advocacy

Introduction



Stuart McClure | CEO / President & Founder

Leader of Cylance as CEO & Visionary

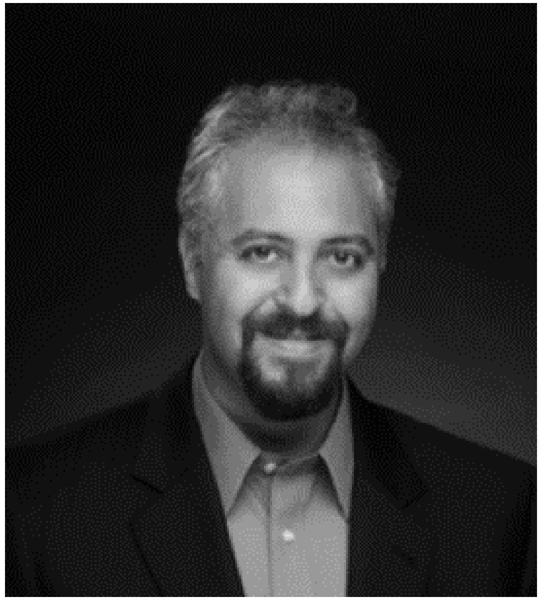
Hacking Exposed

- Lead Author
- Creator
- Most Successful Security Book of All Time

Foundstone

WW-CTO McAfee

Introduction



Ryan Permeh | Co-Founder & Chief Scientist

THE brain behind the mathematical architecture and new approach to security.

Eeye Retina

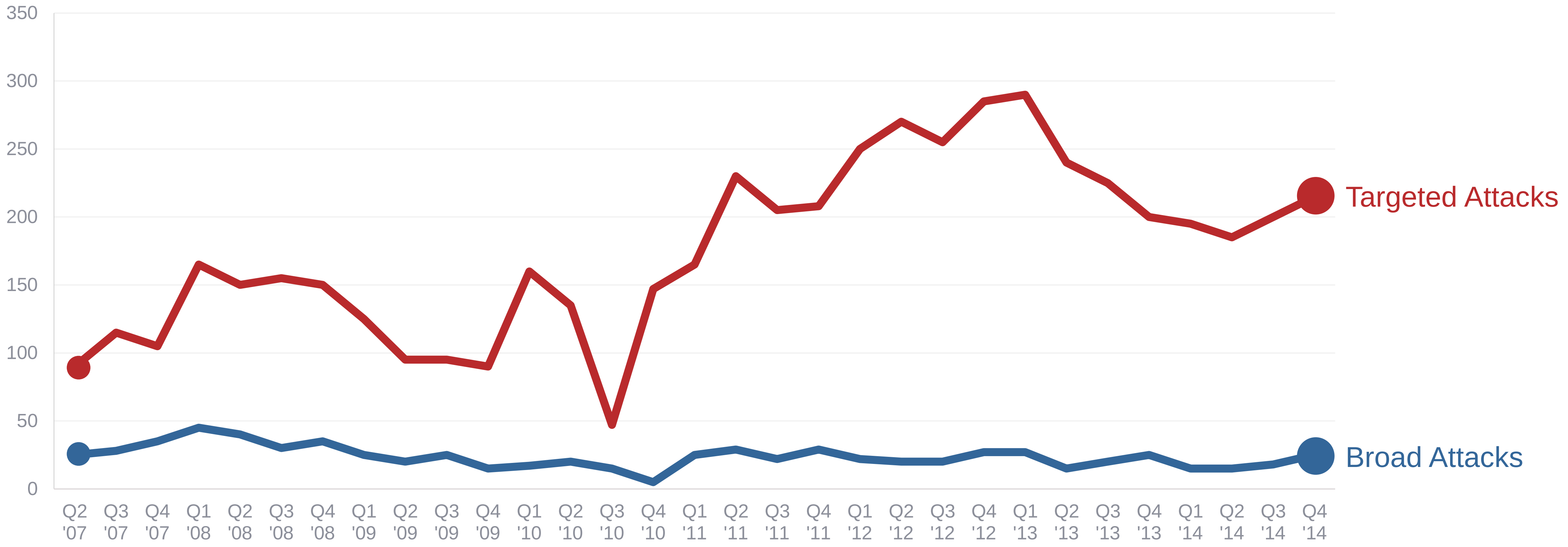
Securells

Code Red

McAfee
Chief Scientist

What is the Problem?

The Rise of Targeted Attacks



Source: CyberFactors, a subsidiary of CyberRisk Partners and CloudInsure.com
http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014

What is the Problem?

Adversaries

Traditional Adversaries

Nation State

- Intelligence
- Intellectual Property Theft
- Espionage

Organized Crime

- Financial Gain
- Identity Theft

What is the Problem?

Adversaries

Next Generation Adversaries

Rogue Nation States

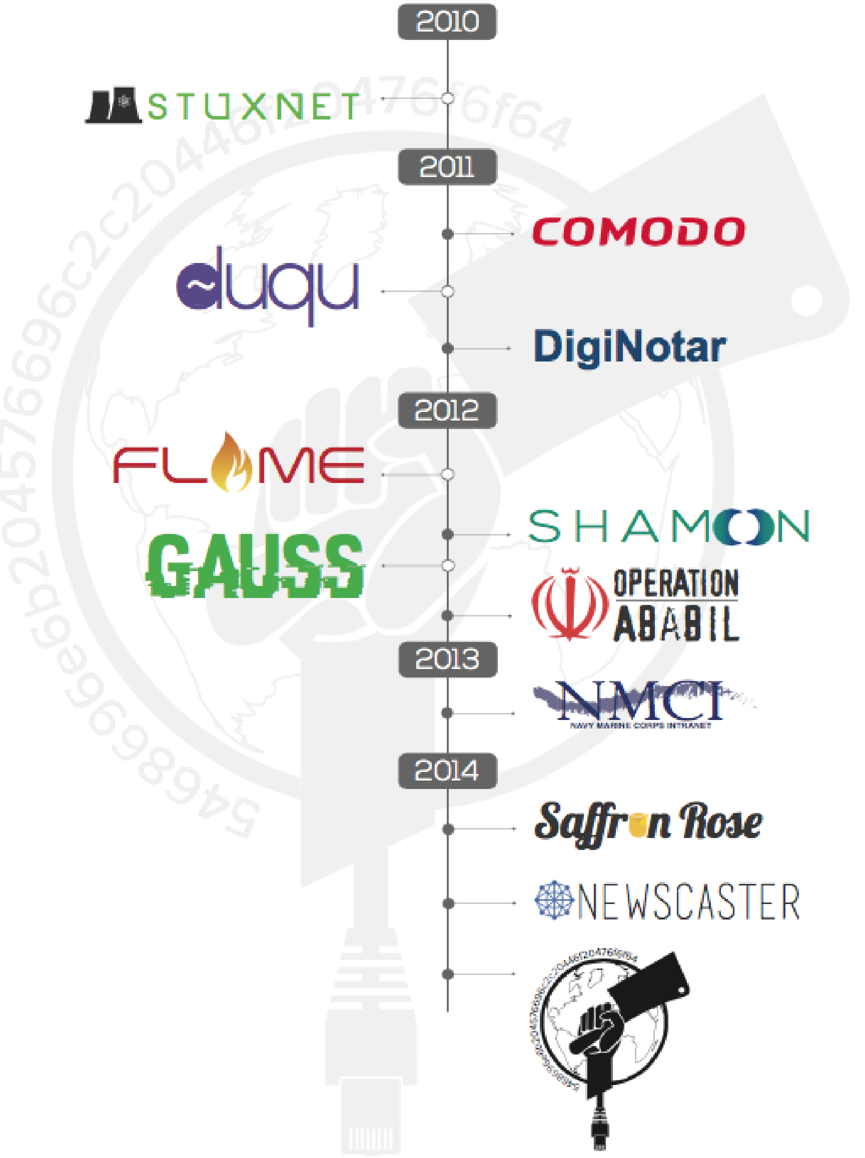
- Iran
- North Korea
- Syria

Individual & Terrorist Actors

- ISIS
- Anonymous
- Etc

Timeline

ORIGINATION RETALIATION



WHY THE NAME CLEAVER?

The string `cleaver` is found several times in a variety of custom software used in Operation Cleaver, including:

1 Numerous references inside the namespaces of their custom bot code codenamed TinyZBot, e.g.:

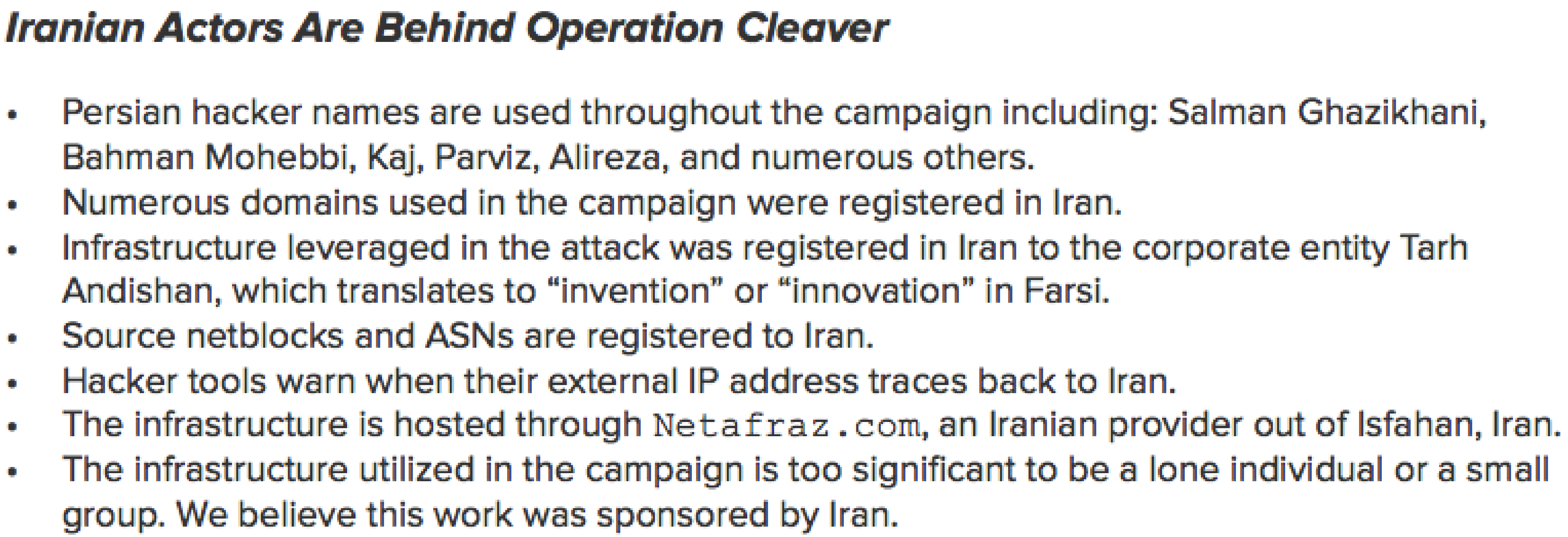
```
e:\projects\cleaver\trunk\zhoupin_cleaver\obj\x86\release\netscp.pdb
```

2 PDBs associated with the hacker name “Jimbp”, e.g.:

```
c:\users\jimbp\desktop\binder_1 - for cleaver\binder_1\obj\x86\release\setup.pdb
```

3 PDBs associated with the keystroke loggers, artifacts, and numerous other tools, e.g.:

```
e:\Projects\Cleaver\trunk\MainModule\obj\Release\MainModule.pdb
```



Iranian Actors Are Behind Operation Cleaver

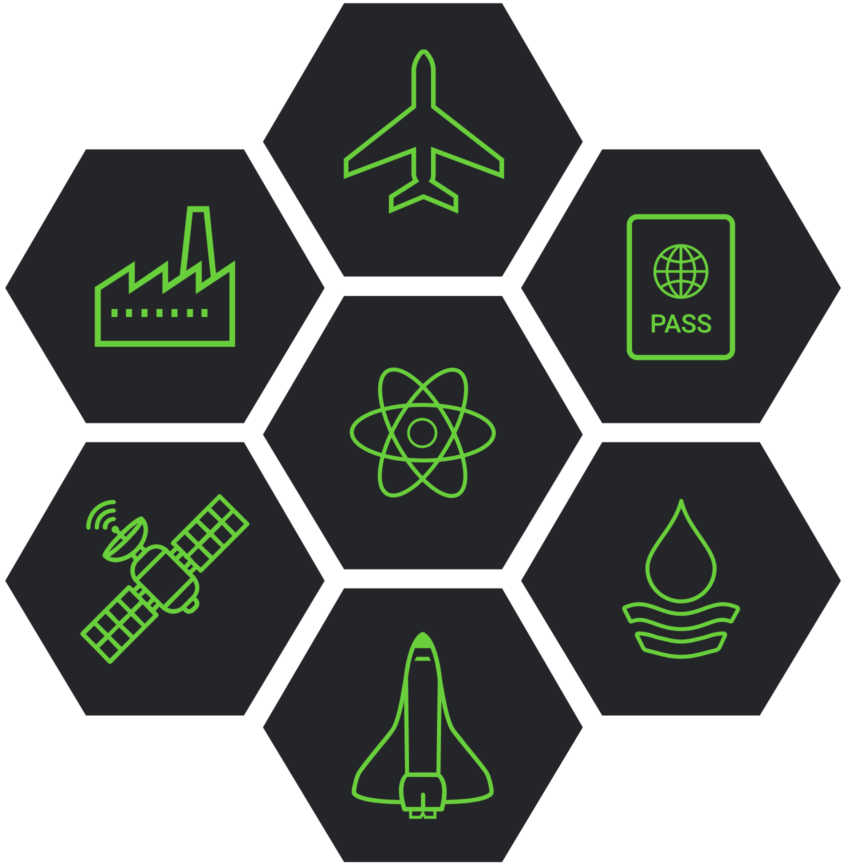
- Persian hacker names are used throughout the campaign including: Salman Ghazikhani, Bahman Mohebbi, Kaj, Parviz, Alireza, and numerous others.
- Numerous domains used in the campaign were registered in Iran.
- Infrastructure leveraged in the attack was registered in Iran to the corporate entity Tarh Andishan, which translates to “invention” or “innovation” in Farsi.
- Source netblocks and ASNs are registered to Iran.
- Hacker tools warn when their external IP address traces back to Iran.
- The infrastructure is hosted through `Netafraz.com`, an Iranian provider out of Isfahan, Iran.
- The infrastructure utilized in the campaign is too significant to be a lone individual or a small group. We believe this work was sponsored by Iran.

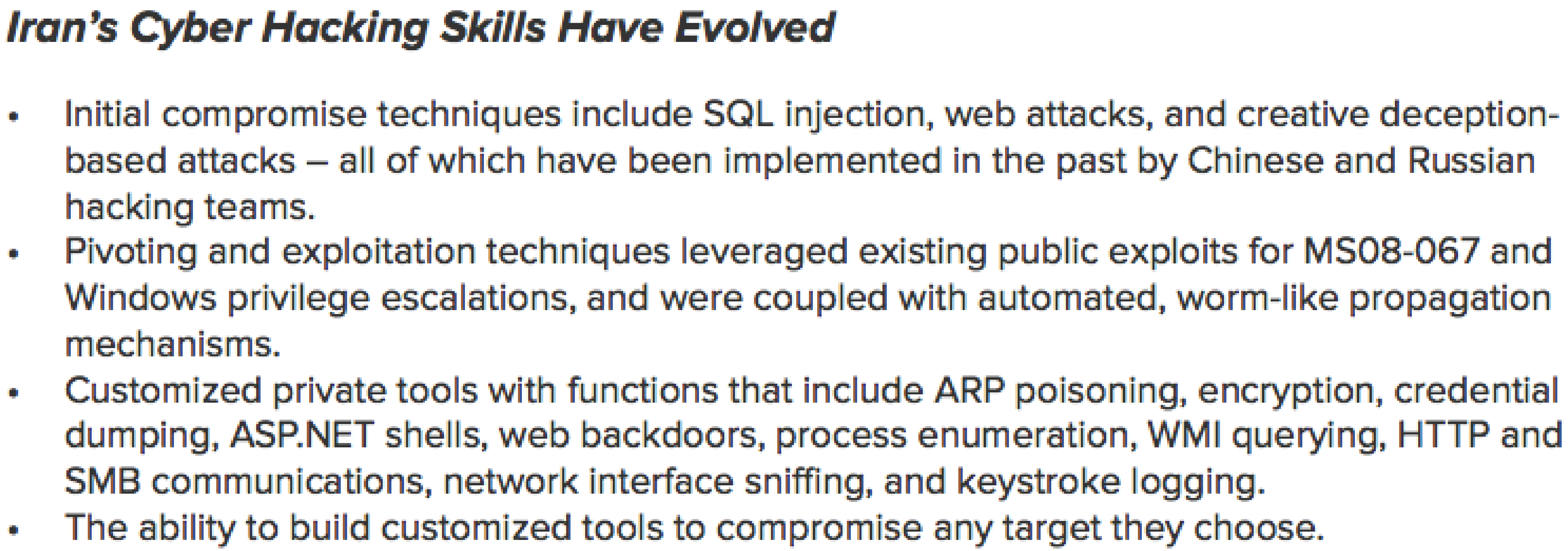
Operation Cleaver

Prevention is Everything

18-24 Month Long
Iranian Offensive

Solely Targeted at Global Critical Infrastructure Companies	Zh0up!n Exploit Team
Phish Based Malware Delivery MS08-067 Pivoting	Public Tools (psexec, mimikatz, cain + abel, etc)
SQL Injection ASP Backdoors Cred Harvesting	Evolved into Using Their Own Zeus Variant (tiny_zbot)



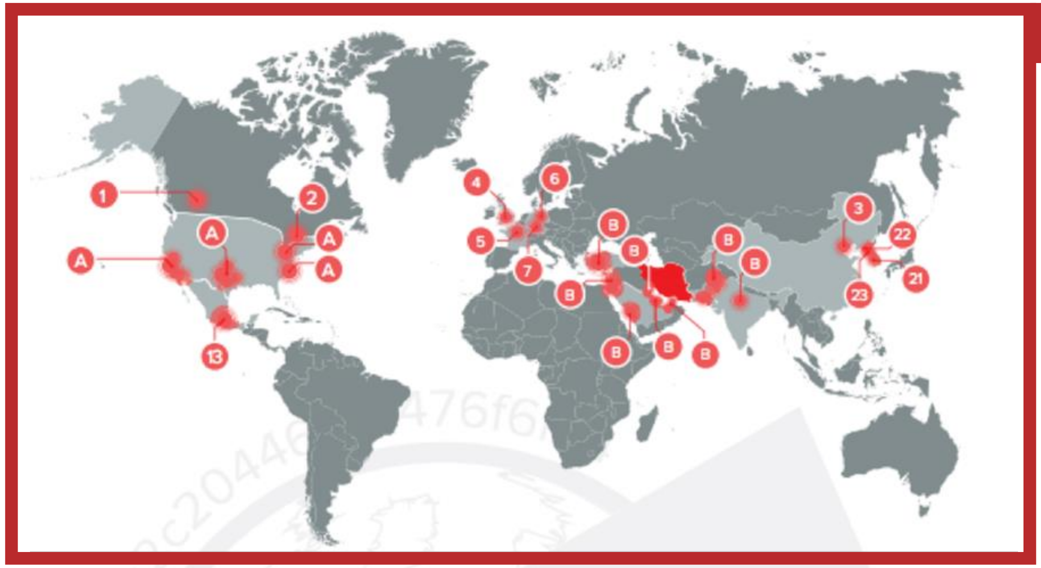


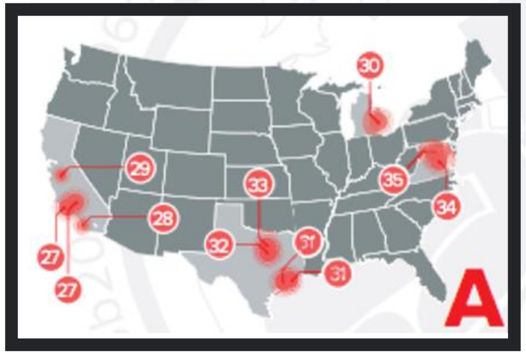
Iran's Cyber Hacking Skills Have Evolved

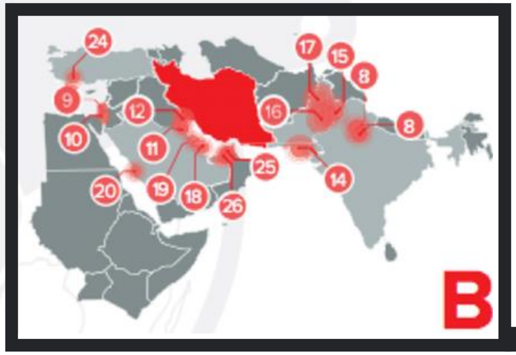
- Initial compromise techniques include SQL injection, web attacks, and creative deception-based attacks – all of which have been implemented in the past by Chinese and Russian hacking teams.
- Pivoting and exploitation techniques leveraged existing public exploits for MS08-067 and Windows privilege escalations, and were coupled with automated, worm-like propagation mechanisms.
- Customized private tools with functions that include ARP poisoning, encryption, credential dumping, ASP.NET shells, web backdoors, process enumeration, WMI querying, HTTP and SMB communications, network interface sniffing, and keystroke logging.
- The ability to build customized tools to compromise any target they choose.

Operation Cleaver

16 Countries Targeted







Canada
- Energy & Utilities
- Oil & Gas
- Hospitals

China
- Aerospace

England
- Education

France
- Oil & Gas

Germany
- Telecommunications

India
- Education

Israel
- Aerospace
- Education

Kuwait
- Oil & Gas
- Telecommunications

Mexico
- Oil & Gas

Pakistan
- Airports
- Hospitals
- Technology
- Airlines

Saudi Arabia
- Oil & Gas
- Airports

South Korea
- Airports
- Airlines
- Education
- Technology
- Heavy Manufacturing

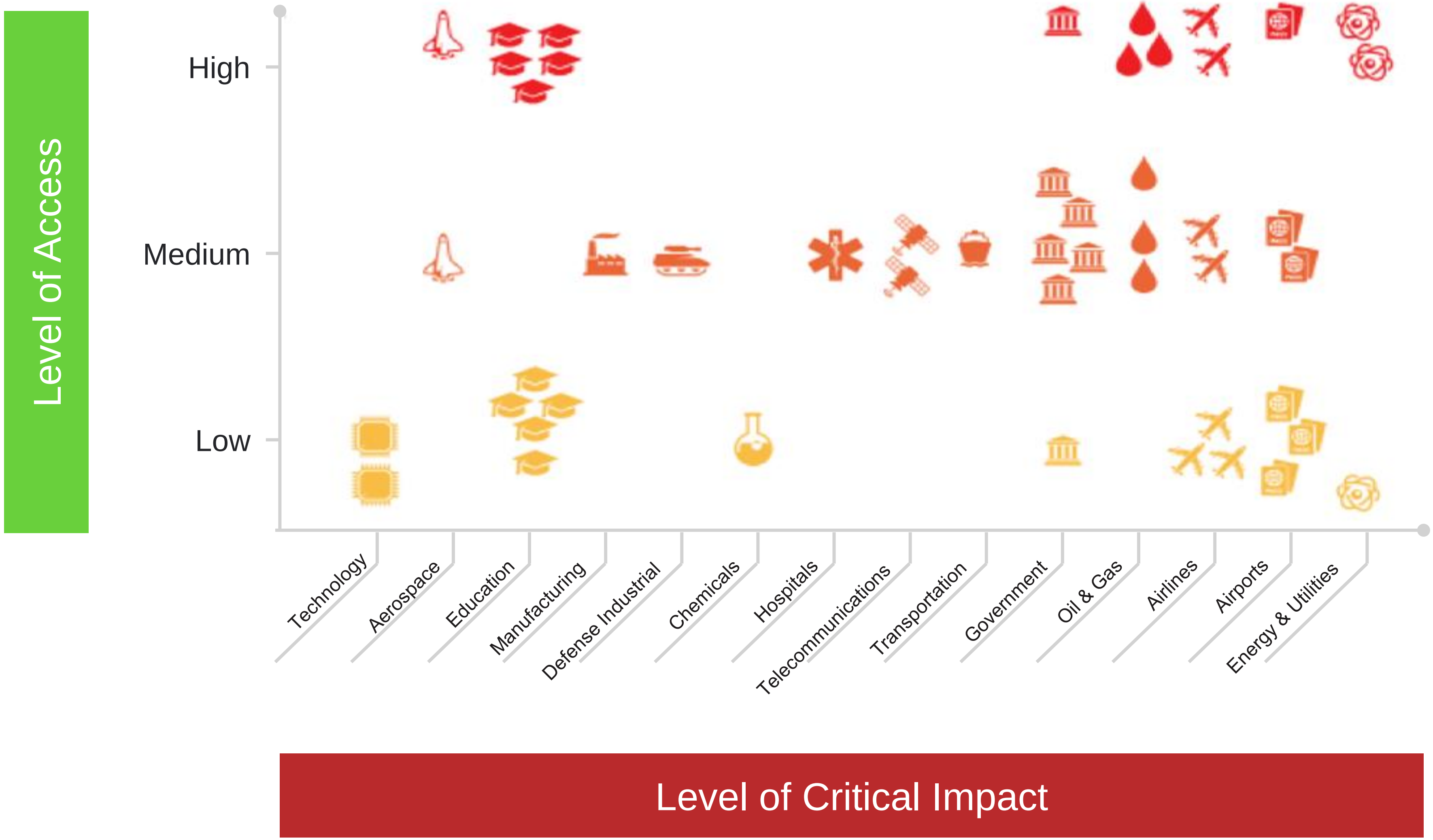
Turkey
- Oil & Gas

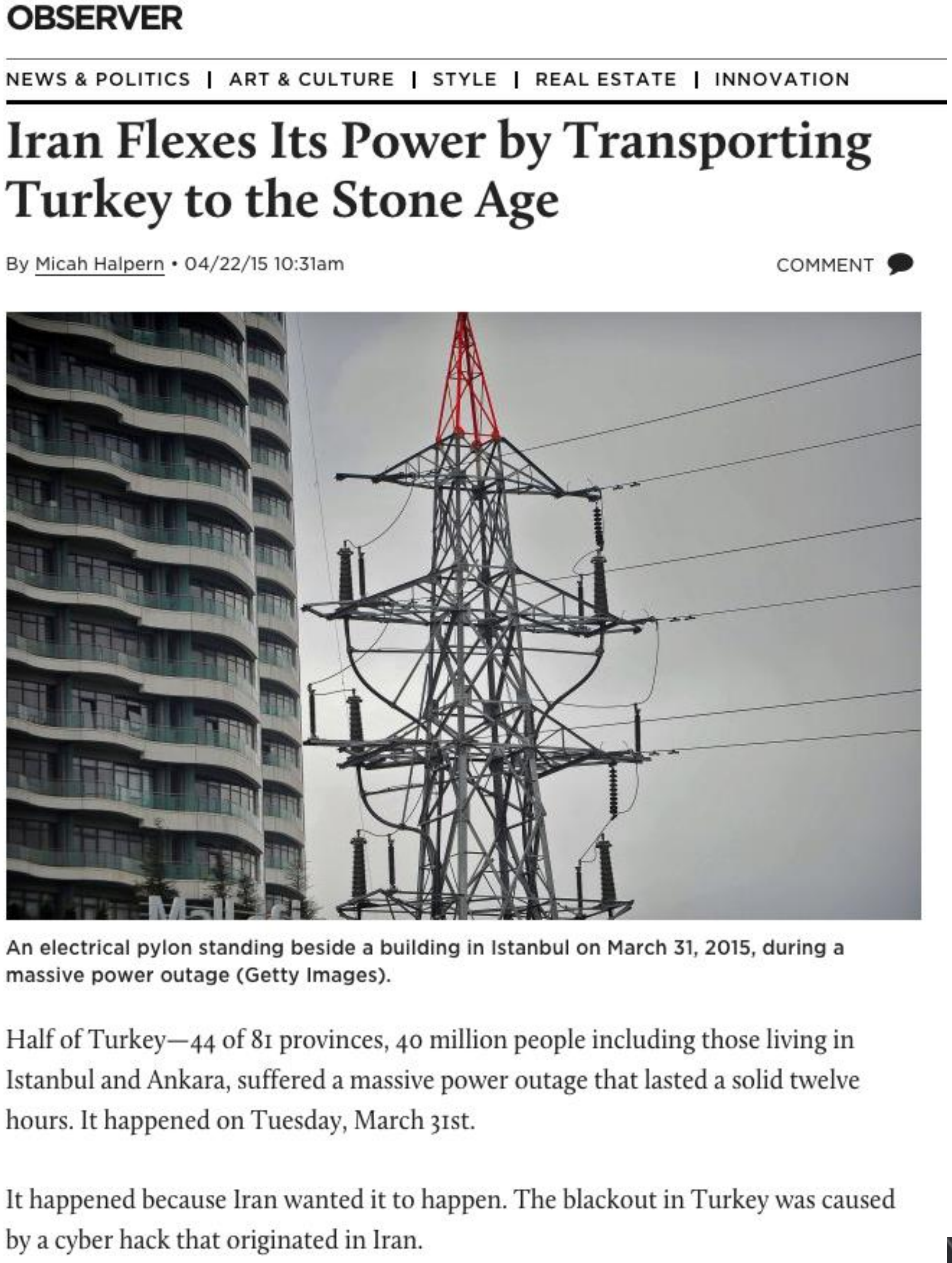
United Arab Emirates
- Government
- Airlines

United States
- Airlines
- Education
- Chemicals
- Transportation
- Energy & Utilities
- Military / Government
- Defense Industrial base

Operation Cleaver

Critical Industries Targeted





OBSERVER

NEWS & POLITICS | ART & CULTURE | STYLE | REAL ESTATE | INNOVATION

Iran Flexes Its Power by Transporting Turkey to the Stone Age

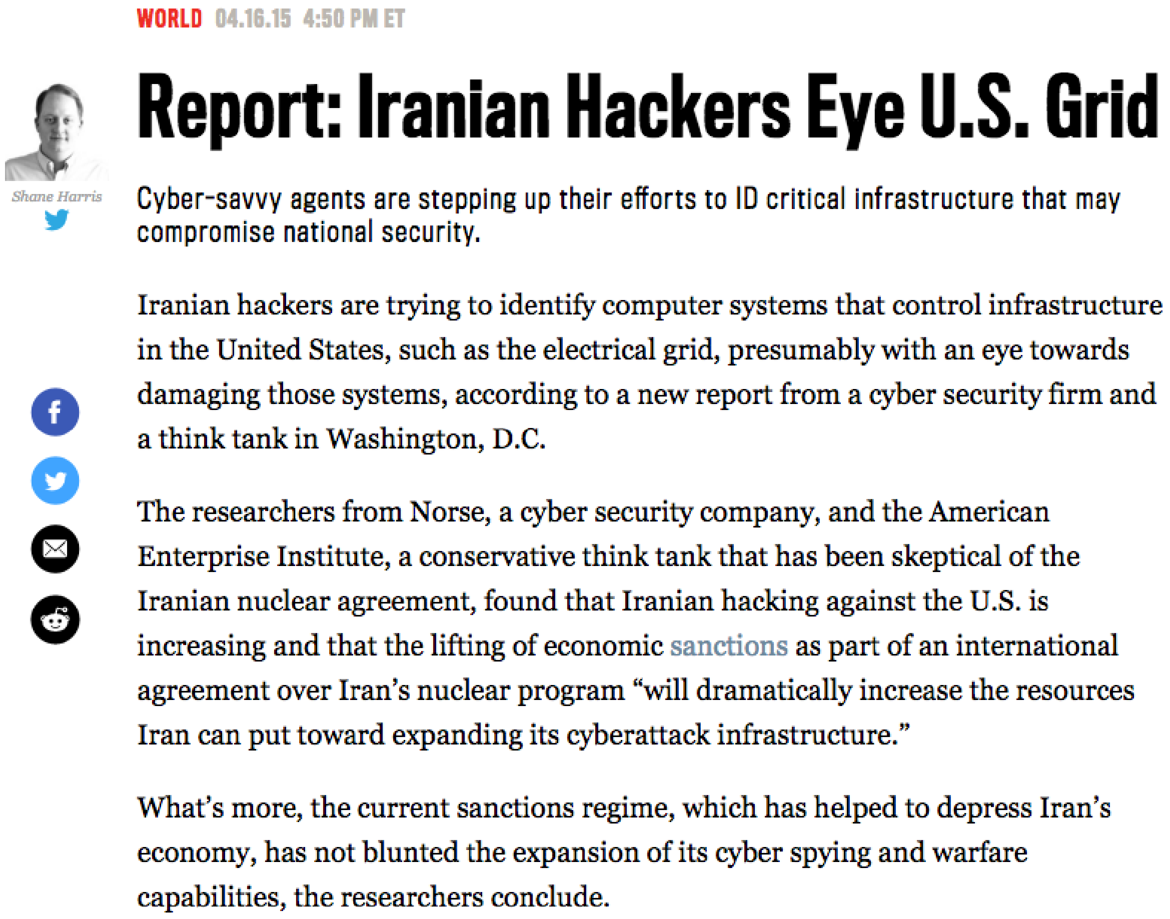
By Micah Halpern • 04/22/15 10:31am

COMMENT

An electrical pylon standing beside a building in Istanbul on March 31, 2015, during a massive power outage (Getty Images).

Half of Turkey—44 of 81 provinces, 40 million people including those living in Istanbul and Ankara, suffered a massive power outage that lasted a solid twelve hours. It happened on Tuesday, March 31st.

It happened because Iran wanted it to happen. The blackout in Turkey was caused by a cyber hack that originated in Iran.



WORLD 04.16.15 4:50 PM ET

Shane Harris

Report: Iranian Hackers Eye U.S. Grid

Cyber-savvy agents are stepping up their efforts to ID critical infrastructure that may compromise national security.

Iranian hackers are trying to identify computer systems that control infrastructure in the United States, such as the electrical grid, presumably with an eye towards damaging those systems, according to a new report from a cyber security firm and a think tank in Washington, D.C.

The researchers from Norse, a cyber security company, and the American Enterprise Institute, a conservative think tank that has been skeptical of the Iranian nuclear agreement, found that Iranian hacking against the U.S. is increasing and that the lifting of economic sanctions as part of an international agreement over Iran's nuclear program "will dramatically increase the resources Iran can put toward expanding its cyberattack infrastructure."

What's more, the current sanctions regime, which has helped to depress Iran's economy, has not blunted the expansion of its cyber spying and warfare capabilities, the researchers conclude.

Questions?

CYLANCE