RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **KEY-T02S**

Global Threat Brief: Hacks and Adversaries Unveiled

Dmitri Alperovitch

Executive Chairman
Silverado Policy Accelerator
@DAlperovitch

Sandra Joyce

Executive Vice President
Mandiant Intelligence
@JumpForJoyce

Russian Invasion of Ukraine

Russian I/O Ineffective

- Secondary Infektion
- Ghostwriter
- Focused on Global South
- Narratives to demoralize & divide Ukrainians and their allies, bolster Russia

Ukraine Is Winning the I/O War

- Zelensky videos
- Civilian cell phones
- Battlefield footage
- Social media
- Hero narratives:
  Snake Island, Ghost of Kyiv

How IR Is Done Under Air Bombardment

"There is no electricity right now, I'll write as soon as the power is back"

"Can we continue tomorrow as one of the main backend developer is at the bomb shelter at the moment"

"this IP-address connected from the temporary occupied territory so it was blocked"

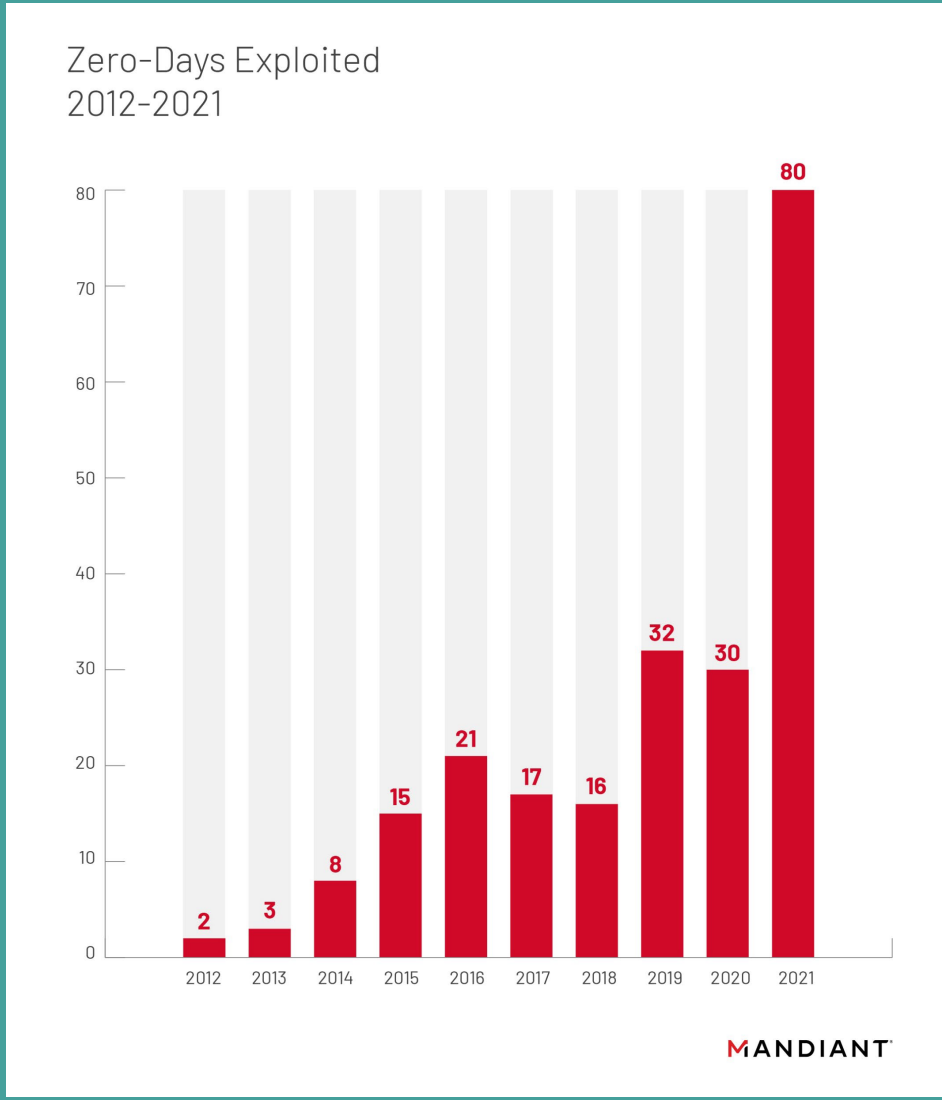
Russia: Defender Takeaways

- Resiliency is key. Learn from Ukraine!
- Don’t be scared of I/O
- SHIELDS UP by CISA

China: Owning the World's Telcos

- LightBasin / UNC1945
  - Linux/Solaris/EulerOS (Huawei) implants
  - Telco focus
  - GPRS protocol for C2
  - Most prevalent zero-day actor
- Increased targeting of State Governments

China: Zero Days



China responsible for 10% of all new zero days exploited in 2021

REAL PROTEST

ALTERED IMAGE

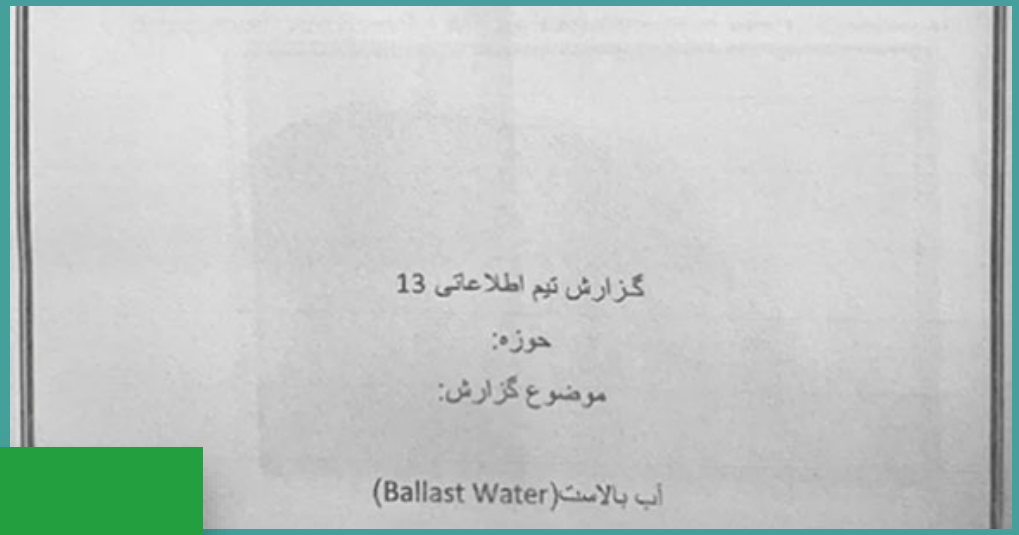

而爆发的区域“恰巧”与美军生物实验室所在地高度吻合
that "happen" to coincide with the location of the U.S. biological laboratory

China: Defender Takeaways

- Inspect non-IP protocols!
- Accelerate patching processes

Iran: Ransomware as Harassment

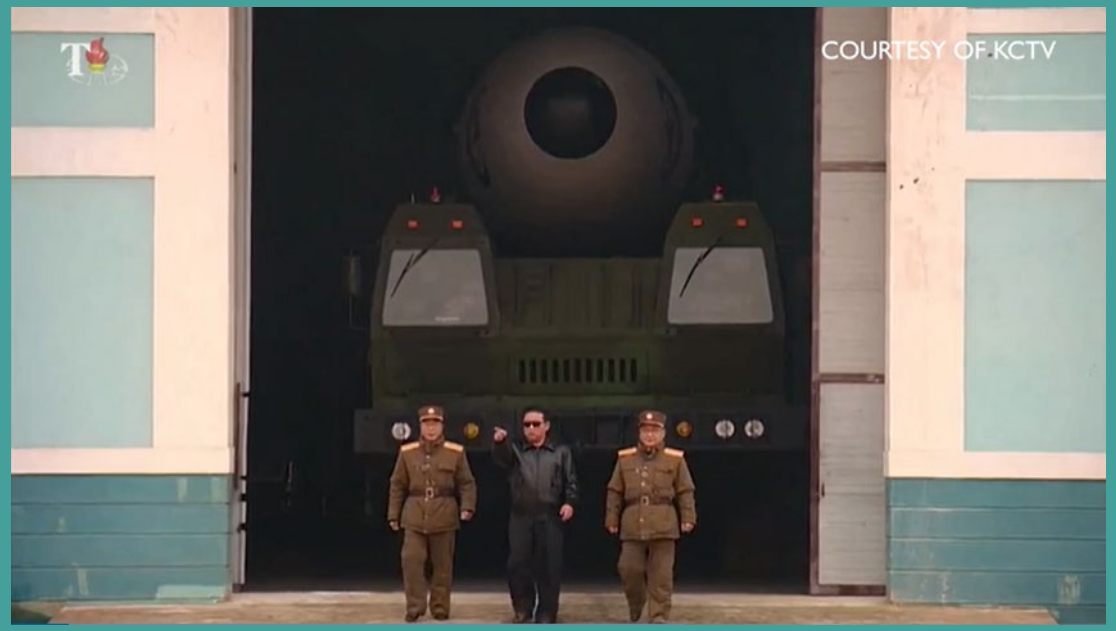
- Government-backed ransomware
  - SamSam was the big innovator
- ICS focus
- Aggressive I/O with combined hack and leak



Iran: Defender Takeaways

- ICS is the next frontier
- Prepare your organizations for leaks. Resilience for leaks!

North Korea: We are BAAAACK



- Insider infiltration from ‘Bay Area’
  - Stolen ID cards
  - Interviews are challenging…
- DPRK coin

Crypto/ Blockchain Business

Crypto/ Blockchain Users

Native Crypto Schemes

IT Outsourcing

Ransomware

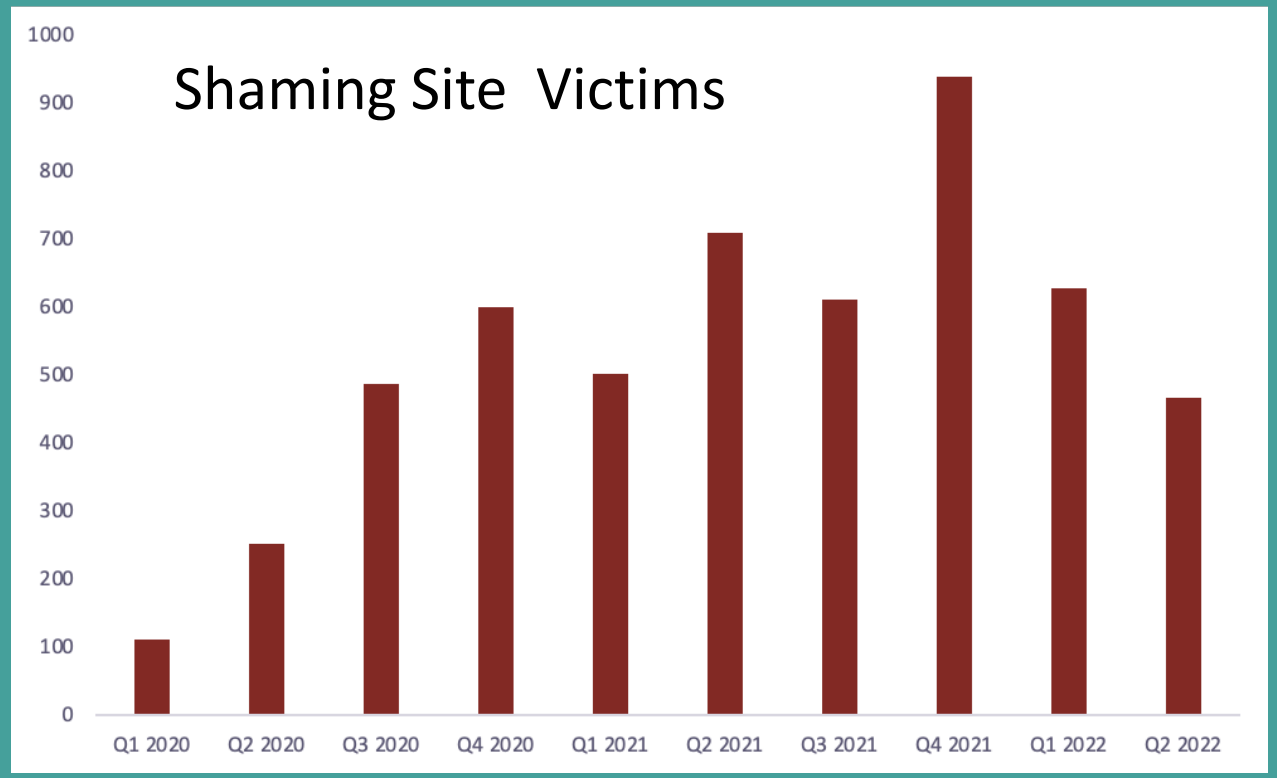
Financial Targeting

North Korea: Defender Takeaways

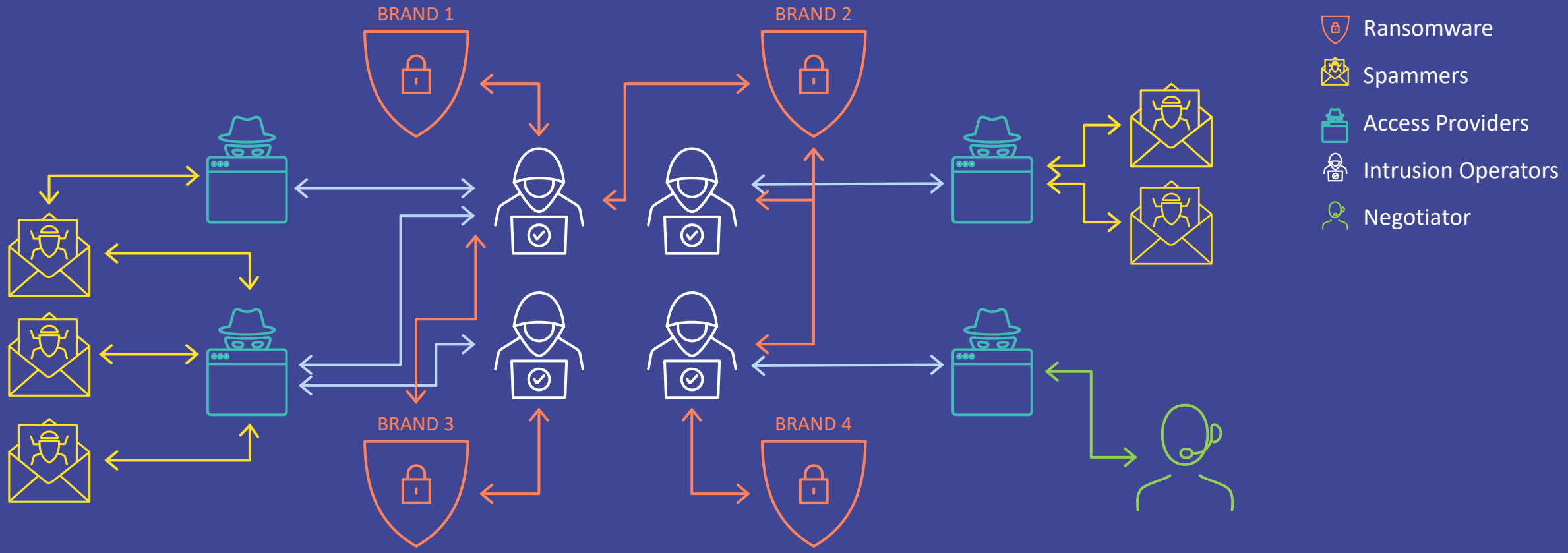
- Beef up your Insider Threat program
- Background checks on contractors. Educate your recruiters
- Crypto businesses: cold storage for wallets is a must!

Crime

- Ransomware cases increasing
- Data Theft & Extortion without ransomware
- Sanctions evasion tactics



A Resilient Ecosystem



Crime: Defender Takeaways

- Have a plan! Don’t panic
- Have IR & negotiator teams on retainers
- Expect leaks
- Practice, practice, practice!

Rise of Hackers for Hire

- Israel: NSO, Candiru, Black Cube, luehawk CI, Intellexa
- India: BellTroX
- Macedonia: Citron
- US/UAE: Darkmatter
- China

Hackers for Hire: Defender Takeaways

- Don’t give away your cell phone # (use VOIP #s)
- Reboot your phone frequently
- If you are HVT, contact Citizen Lab

RSAConference2022

Strategic Takeaways

Conclusions

- Almost every actor is maturing in I/O space
  - Effectiveness is a question
- Ransomware is here for the long term
- Preparedness, not Panic. Take care of defenders!
- Time to reevaluate cyber warfare assumptions
- The enemy is not 10 feet tall
- The fight is contingent

RSAConference2022

Thank you!

@Dalperovitch

@JumpForJoyce