Real Breach Stories
from the
Trenches

Ondrej KREHEL
Elite Cyber Team with Military Approach
"Let There Be a Code"
Cyber extortion

- Ransomware
- Service disruption - DDoS
- Sextortion
- Executives and officers
- Teenagers and mobile
- Payroll data and systems
- After breach clean-up
FBI wants U.S. businesses to help as cyber extortion gains urgency

BY JIM FINKLE
Cyber’s Most Wanted

Select the images of suspects to display more information.

- IRANIAN DDoS ATTACKS
- FIRAS DARDAR
- AHMED AL ACHHA
- EVGENY MIKHAILOVICH BOUSACHEV
- JOSHUA SAMUEL AARON
- RUCHEN GANEN
- ZHENGZHOU JIANYI
- SUN KAIJANG
- HUANG ZHENYU
- WEN XINYU

On January 21, 2016, a grand jury in the Southern District of New York indicted seven Iranian nationals for their involvement in conspiracies to conduct a coordinated campaign of distributed denial of service (DDoS) attacks against the United States financial sector and other United States companies from 2011 through 2015. Each defendant was a manager or employee of SimSoc Team or Mersad, private security computer companies based in the Islamic Republic of Iran that performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps.
How Do You Know When You Are Hacked?
What Should You Do When You Are Hacked?

KEEP CALM AND UPDATE YOUR RESUME
Q & A

Tim, did you read the latest CyberNews yet?

Of course! I just signed up for free! Good content and funny jokes, I love it!

Sign up for CyberNews: LIFARS.com/cybernews
REAL BREACH STORIES FROM THE TRENCHES: COMMUNICATIONS IMPERATIVES

August 18, 2016
Edelman’s Data Security & Privacy Group

- **Strong understanding of the security landscape** through our work with leading technology, cyber-forensics and privacy organizations

- **Dedicated Data Security & Privacy Crisis Communications** team with years of experience helping companies handle the most complex reputation challenges

- **Experience** managing a range of security issues from vulnerabilities in products to data breaches in major industries including healthcare, financial services and retail

- Global footprint with **privacy and security communications experts** based around the world who understand local laws and culture

- Experience working with **leading law firms, forensics firms and data breach resolution providers**
Communications Imperative #1: The Early Bird Doesn’t Always Catch The Worm

• Move quickly … but remember that in a data breach going out with information too early can hurt an organization

• “Facts” are very fluid - so rushing public statements can result in a number of bad outcomes for a company

Edelman in Action

• Engaged by major health insurer in Q1 2015 to provide communications support in response to a cyberattack that compromised the financial and medical information of 10 million+ current and former members

• Encouraged organization to resist the urge to communicate too far in advance of complete network remediation and focus on a long-term strategy

• Helped company protect short-term license to operate and mitigate long-term damage to the brand

The New York Times
For Target, The Breach Numbers Grow
Edelman in Action

Hired by one of the country’s largest public universities in Q1 2016 to help manage expansive cyber-attack, resulting in lost social security numbers and other PII for tens of thousands of past and present students and employees.

Prepared multi-channel approach to communications, including dedicated microsite.

Helped limit news cycle to within nearly one week of the disclosure.

Communications Imperative #2: Customers Must Be Your North Star

- Manage the message through traditional and digital channels
- Be accountable, not the victim
- Regain trust by demonstrating a bias toward action
Communications Imperative #3: Take The Oxygen Out Of The Media Fire

- Avoid amplifying the story or inadvertently creating additional news cycles through multiple/conflicting statements
- Set up the appropriate media/social monitoring and listening posts
- Think through planned content on social media

Engaged by major Midwest hospital that experienced computer security incident involving the personal and health information of patients, providers and employees

Provided on-site counsel and support to manage announcement day communications and media relations

Transactional approach to media resulted in minimal Day 1 news coverage and no on-site media
Communications Imperative #4: Employees Are Your Most Credible Spokespersons; Keep Them Informed

“Me to We”: Addressing concerns and engaging employees in the solution

Edelman in Action

- Worked with major health insurer that experienced cyberattack to develop a robust internal communications strategy.
- Developed internal video from the company CEO to communicate with employees.
- Helped to rally employees and equip them to be credible spokespersons for the company.
Communications Imperative #5: Fail To Plan … Plan To Fail

**ANALYZE & ASSESS RISK**
Assess any current crisis plans and protocols as well as the company’s current privacy and security protocols; identify gaps and areas of opportunity.

**BUILD INCIDENT RESPONSE PLAN**
Create a purpose-built crisis preparedness plan that identifies team roles and responsibilities, explores key response scenarios and includes sample messaging along with forms and checklists to ensure rapid response capability.

**TEST THE PROCESS**
Pressure test the plan and team through simulating a priority risk scenario, such as a data breach; identify gaps and areas for improvement.

**OPERATE AND MANAGE**
Activate 24/7 crisis response as needed.
Real Breach Stories from the Trenches:
Notification and Remediation
Notification and Remediation

- **Data Breach**
  - Forensics: Identify cause and extent of breach, Minimize impact, Recommendations to prevent future exploitation
  - Print/Mail House: Letter preparation, Printing, Mailing, Tracking, Reporting
  - Call Handling: Toll-free number, Dedicated fraud specialists, Identify special handling needs, Call center metrics
  - Remediation: Credit / Identity monitoring services, Credit file reviews, Place fraud alerts, Victim resolution services, Post fraud follow-up, Comprehensive case files

Holistic In-House Breach Response Services

Resolution
Contact Information

Rich Blumberg
Director, Data Breach Response
IDT911
E: rblumberg@idt911.com
O: 404-227-2963

Jamie Singer
Senior Account Supervisor
Crisis & Risk Management,
U.S. Data Security & Privacy Group
Edelman
E: Jamie.Singer@Edelman.com
O: 312.240.2657

Ondrej Krehel
Founder and CEO
LIFARS, LLC
E: Ondrej.Krehel@lifars.com
O: 212-222-7061