Barbarians Inside the Firewalls: Cybersecurity for Small Business

May 1, 2019

Presented by:
Jon Neiditz
Doug Gilfillan
Presenters

Jon Neiditz
Partner, Atlanta
jneiditz@kilpatricktownsend.com

Jon Neiditz co-leads the Cybersecurity, Privacy and Data Governance Practice at Kilpatrick Townsend. One of the first lawyers to focus broadly on data governance and knowledge asset protection, he remains the only person recognized by Best Lawyers in America® both for Information Management Law and for Privacy and Data Security Law. For decades Jon has helped clients anticipate, obviate, and manage information privacy and security risks; appropriately monetize information; comply with privacy, data protection and cybersecurity laws around the world in pragmatic ways; and contain and prevent harm from incidents while maximizing resilience and recovery afterwards. Jon was selected as a “Cybersecurity Trailblazer” by the National Law Journal and as a Ponemon Fellow. Jon is certified by the IAPP in Europe as well as in the U.S. (CIPP/E, CIPP/US and CIPM).

Doug Gilfillan
Partner, Atlanta
dgilfillan@kilpatricktownsend.com

Doug Gilfillan focuses his practice on white collar criminal defense, cyber-crime and data breach responses, grand jury investigations, government regulatory investigations and enforcement actions, internal investigations, and complex civil litigation. A former federal prosecutor, Doug has acted as lead counsel and tried numerous cases to jury verdict in a wide variety of white collar criminal cases. Prior to joining the firm, Doug served in the United States Attorney’s Office for the Northern District of Georgia, where he supervised and handled a wide variety of white collar criminal investigations and prosecutions. Most recently, Doug was Chief of the Cyber Crimes and Intellectual Property Section and National Security Cyber Specialist in the United States Attorney’s Office for the Northern District of Georgia.
Cyber-Threats Hit Businesses of All Sizes

You don’t have to be a target; malware is crawling all systems

All systems are vulnerable and most are infected

Once you click, out jumps the cybercriminal, who can begin “living off the land”
Effective because:

• Low barriers to entry – requires little technical expertise

• Lack of fixed location
  – Cybercriminals reach across the world and commit crimes in multiple jurisdictions

• Anonymity – criminals can easily adopt alter egos and conceal their tracks
  – Multiple participants (or not?)

• Extradition treaties
  – Criminals hide behind legal barriers to apprehension

• Human psychology - trust, naivety, hope and greed
Cybercrime cost businesses a record $2.7 billion in 2018, nearly double the $1.4 billion reported a year earlier.

Source: FBI, April 22, 2019

Common types of for-profit cybercrime

- Fraud
- Phishing & spearphishing
- Identity theft
- Social engineering (using data gleaned from social media)
- Business email compromise
- Data breaches
- Ransomware
Suddenly, your system goes down. You call IT, who’s not sure what it is.

– Who do you call?
– What does the down-time mean for your business?
– Cloud or local systems?
Hello, Women In Distress!

Check this message in details and contact someone from IT department. All your files are encrypted. Don't modify encrypted files because this may cause decryption failure.

If you want to restore your files you will need to make the payment. Otherwise your files will be shared in the Internet which may lead you to the loss of reputation.

You can send us an encrypted file (about 100KB) and we will decrypt it for free. The file will help us to resolve doubts in possibility to restore the files any time.

Contact us only if you are authorized to make a deal from the whole affected network.

This file generation date (month/day/year): 03/18/2019.

I note that every 5 days initial ransom price will be raised.

Email address and BitMessage identity would be actual for the next 2 weeks, don't waste time and contact us as soon as possible.
Ransomware Fire Drill

- What are always the biggest, first issues with ransomware?
- Who is now participating?
- Who’s making the decisions?
- What’s happening to stop spread (containment)?
- Is law enforcement involved?
- Can you get quick access to cryptocurrency?
- Who will communicate with the bad guys?
- Who will decide about payment?
# To Pay or Not to Pay in Any Availability Attack

<table>
<thead>
<tr>
<th>Do Not Pay</th>
<th>Pay</th>
<th>Wait to Pay</th>
</tr>
</thead>
<tbody>
<tr>
<td>• High confidence in backups</td>
<td>• Impact to critical systems/data</td>
<td>• Evaluate threat</td>
</tr>
<tr>
<td>• High confidence in restoration time</td>
<td>• Unable to respond/recover</td>
<td>• Credible?</td>
</tr>
<tr>
<td>• High confidence in Incident Response, Disaster Recovery and/or Business Continuity Plans</td>
<td>• Inadequate or infected backups</td>
<td>• Reversible?</td>
</tr>
<tr>
<td>• Low likelihood of propagation</td>
<td>• No known vulnerabilities in encryption mechanism/ inability to recover</td>
<td>• Conduct triage forensics</td>
</tr>
<tr>
<td>• Low risk/Low impact</td>
<td>• Potential for ransomware variant to propagate throughout enterprise</td>
<td>• How much time did the attackers give? Number of notices?</td>
</tr>
<tr>
<td>• Well defined forensics with a root cause</td>
<td>• Inability to prevent ransomware variant delivery and execution</td>
<td>• Evaluate potential daily loss</td>
</tr>
<tr>
<td>• Good information on the M.O. from law enforcement and forensics</td>
<td>• Unsure of breadth of penetration</td>
<td>• Enterprise-wide?</td>
</tr>
<tr>
<td></td>
<td>• N.B.: No guarantee of getting your data back</td>
<td>• Greater than 1000 Records?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Critical systems/data?</td>
</tr>
</tbody>
</table>
But Wait...There’s More

• While scanning systems for the ransomware, IT discovers a credentials-harvesting Trojan.
  – What should happen immediately?
  – What makes this different than the ransomware?
  – Is your response different than it was to the ransomware?
Forensics, Communication & Remediation

- Forensics and research on the Trojan reveal what was exposed:
  - For Customers: Access credentials, credit card and bank account information
  - For Employees: Personal as well as system log-on credentials and social security numbers
  - Why did you need to research the Trojan?
- With whom to communicate and what do you say?
  - Which notices should be given immediately and which notices must be given?
  - What customer and employee remediation services should be offered?
- What are some of the basics of systems remediation in the ransomware and the breach?
- What are the liability risks and how do you minimize such risks?
Questions?