CHART EXCHANGE

Coverholders And Risk Takers Exchange

Volume 4 • Issue 12
December 2019

Bridging The Gap Between Lloyd's of London And The U.S. Domestic Market

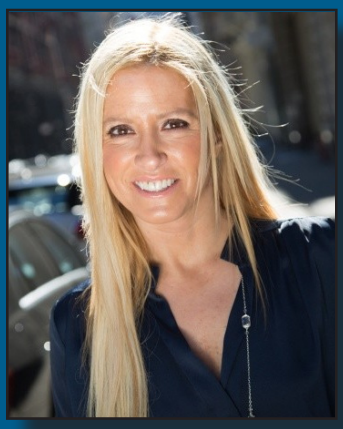
NO PAYMENT? NO PRIVACY: A FRIGHTENING INNOVATION IN RANSOMWARE

By Timothy Lehey and Jennifer Rothstein

Ransomware is a highly technical deployment of an ancient interpersonal crime: extortion. Since its advent, cybercriminal organizations and security personnel continue to play a game of cat and mouse at the front lines of technology. However, as much as the details may change, the core dynamic of this crime remains the same: criminals steal something of great value and demand payment in exchange for its return.

As organizations improve their ability to respond successfully to ransomware attacks, cybercriminals too will change their methods. For example, organizations are increasingly aware of the importance

See Ransomeware Page 32



About the Co-Author: Jennifer Rothstein is the Business Development Head, Insurance & Legal, for BlueVoyant, a cybersecurity provider headquartered in New York City. She also co-founded and serves as the President of Women in Cyber Leadership Corp. As the cyber security industry has been rooted in STEM and the military, she recognized that it can be intimidating for women to start and thrive within the space, and has dedicated her efforts to providing everyone with the tools, opportunity, knowledge and confidence to succeed in cyber.

Throughout her career at companies such as Kroll and AIG, she has lead the effort in combining cyber expertise with her deep knowledge in insurance. She is driven by a resolve to demystify two complex categories allowing access and understanding to both cybersecurity and insurance in our increasingly interdisciplinary and interconnected world.

About the Co-Author: Tim Lehey is a Cyber Threat Intelligence Analyst and Dark Web Investigator at BlueVoyant. He has expertise in open-source and dark web online investigations. Tim holds a Master's in International Security Policy and previously worked as a Latin America Cybercrime Analyst at the dark web intelligence firm Flashpoint.

Continued From Page 16

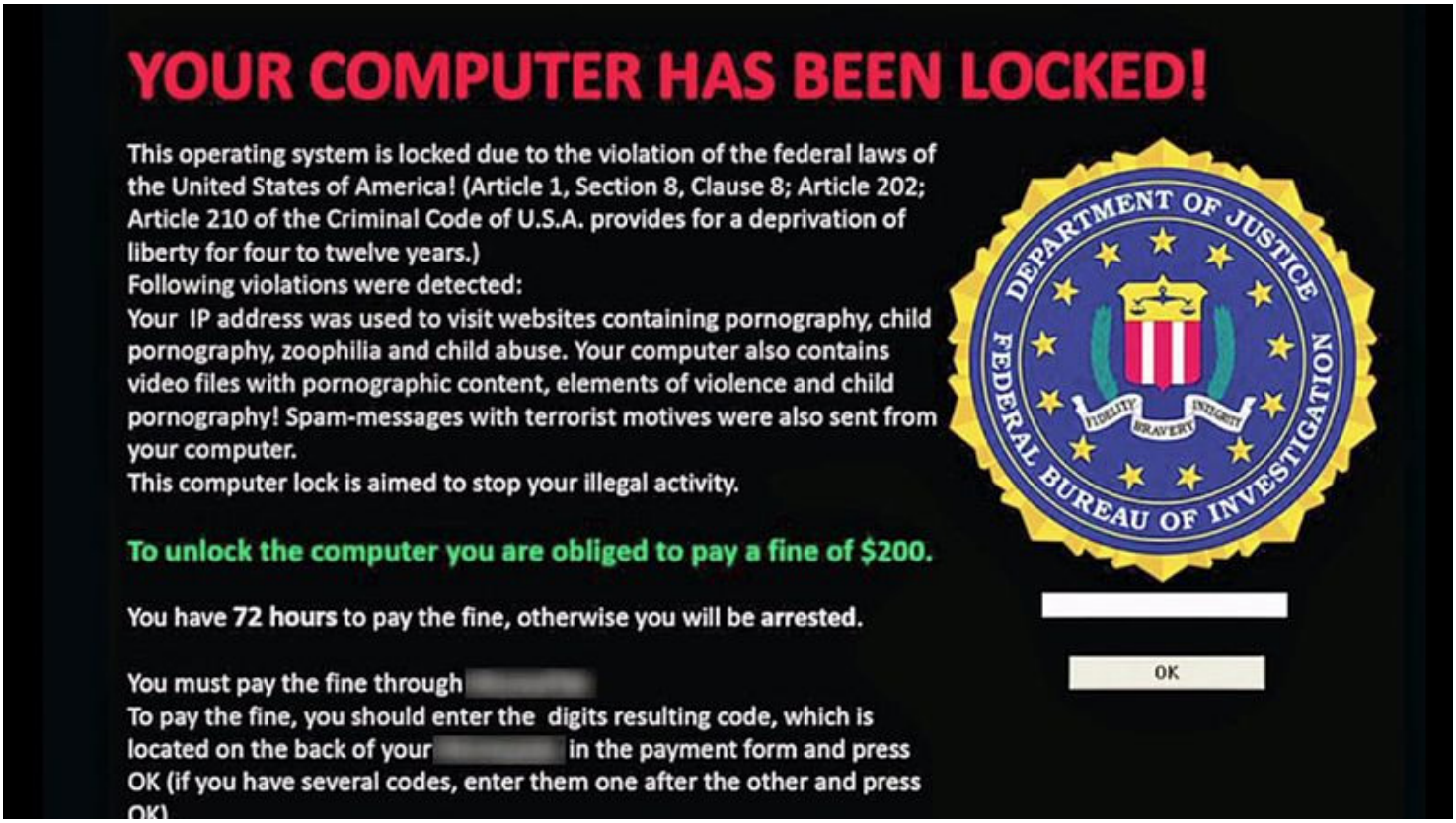
A FRIGHTENING INNOVATION IN RANSOMWARE

of implementing offline, routinely updated system backups. Subsequently, when hit with ransomware, they can ignore demands for ransom and simply restore their operations from backups after wiping everything clean. This is undoubtedly an inconvenience, but far superior to paying several hundred thousand dollars in bitcoin to an undeserving overseas criminal organization.

Threat actors have long tried to foster urgency in their ransom demands. The innovation of countdown clocks within ransom notes was notable. If victims didn't pay within a certain time period – stressfully shown counting down by the minute – the ransom amount would double, then triple, and so on. Now, however, we are seeing an interesting and frightening new development that may represent the cutting edge of ransomware extortion: the leak. There have been no definitively proven cases of this tact so far, but rumors and insinuations suggest there are now ransomware attacks whereby attackers threaten to release sensitive organizational data to the public in order to incentivize swift payment of the ransom.

This strategy may have caused the October intrusion into Johannesburg, South Africa's municipal system, and more recently, news sources reported that the Maze cybercriminal organization leaked 700 MB of data it stole from Allied Universal in November this year. That group

See Ransomware Page 38



Continued From Page 32

A FRIGHTENING INNOVATION IN RANSOMWARE

told cybersecurity researchers they stole 5 GB of Allied Universal's data and they will provision the remainder to Wikileaks if the California-based security firm refuses to pay the 300 bitcoin ransom. Maze are not the only cybercriminals experimenting with this tactic. MegaCortex is a known version of ransomware, however a new variant was recently released that changes passwords on infected machines and threatens to publish the ransomed data if payment isn't made. According to cybersecurity researchers at Bleeping Computer, this is the threat excerpted from the ransom note:

> *"We have also downloaded your data to a secure location. In the unfortunate event of us not coming to an agreement we will have no choice but to make this data public. Once the transaction is finalized all of copies of data we have downloaded will be erased."*

The transition to the threat of publication is key because it undermines the tried and true solution for prepared organizations – data restoration from backups. In this scenario, even if you can wipe and rebuild your system, attackers could potentially still publish your customers' payment card information (PCI), your patients' private health information (PHI), or whatever other sensitive data you may have in your care. These variants also instruct the victim to contact the ransomer for the price of the decryption keys. In theory, an attacker could appraise the value of the exfiltrated data after successfully coercing the victim to the point of negotiation.

At the time of this writing, there is no proof that the exfiltration of data has been successfully implemented in a ransomware scheme, but it remains a troubling possibility. Also, underreporting of events is still a major problem in the field of cybersecurity because of the reputational damage it can unleash, so therefore we may be unaware of the already-successful use of this tactic.

In this evolving game of extortion, data exfiltration and the threat of its release may be the next offensive move by the ransomware criminal enterprise.

References:

1. https://www.bankinfosecurity.com/unwanted-escalation-ransomware-attackers-leak-stolen-data-a-13438
2. https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/
3. https://www.bleepingcomputer.com/news/security/new-megacortex-ransomware-changes-windows-passwords-threatens-to-publish-data/

BlueVoyant

www.bluevoyant.com

- For insureds that need forensics, incident response, or proactive security services
- BlueVoyant is a pure play cybersecurity firm
- **WE GET IT** – we do it faster and better

Austin Berglas | Global Head of Professional Services
austin.berglas@bluevoyant.com

Vincent D'Agostino | Head of Cyber Forensics & Incident Response
vincent.dagostino@bluevoyant.com

Jennifer Rothstein | Business Development Head, Insurance & Legal
jennifer.rothstein@bluevoyant.com

Breached: incident@bluevoyant.com | **Info:** contact@bluevoyant.com