FBI Website

Ransomware attacks are not only proliferating, they're becoming more sophisticated. Several years ago, ransomware was normally delivered through spam e-mails, but because e-mail systems got better at filtering out spam, cyber criminals turned to spear phishing e-mails targeting specific individuals. And in newer instances of ransomware, some cyber criminals aren't using e-mails at all—they can bypass the need for an individual to click on a link by seeding legitimate websites with malicious code, taking advantage of unpatched software on end-user computers.

The FBI doesn't support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee an organization that it will get its data back—there have been cases where organizations never got a decryption key after having paid the ransom. Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals.

So what does the FBI recommend? As ransomware techniques and malware continue to evolve—and because it's difficult to detect a ransomware compromise before it's too late—organizations in particular should focus on two main areas:

- Prevention efforts—both in both in terms of awareness training for employees and robust technical prevention controls; and
- The creation of a solid business continuity plan in the event of a ransomware attack.

Here are some tips for dealing with ransomware (primarily aimed at organizations and their employees, but some are also applicable to individual users):

- Make sure employees are aware of ransomware and of their critical roles in protecting the organization's data.
- Patch operating system, software, and firmware on digital devices (which may be made easier through a centralized patch management system).
- Ensure antivirus and anti-malware solutions are set to automatically update and conduct regular scans.
- Manage the use of privileged accounts—no users should be assigned administrative access unless absolutely needed, and only use administrator accounts when necessary.
- Configure access controls, including file, directory, and network share permissions appropriately. If users only need read specific information, they don't need write-access to those files or directories.
- Disable macro scripts from office files transmitted over e-mail.
- Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations (e.g., temporary folders supporting popular Internet browsers, compression/decompression programs).
- Back up data regularly and verify the integrity of those backups regularly.
- Secure your backups. Make sure they aren't connected to the computers and networks they are backing up.

Financial Fraud Kill Chain

Federal Bureau of Investigation
11 January 2016

Criminal actors are laundering billions of dollars overseas through financial fraud schemes like corporate account takeovers, business e-mail compromise scams, and other financially motivated crimes. The Financial Fraud Kill Chain (FFKC) is a process for recovering large international wire transfers stolen from US victim bank accounts. The FFKC utilizes FINCEN's relationship with the Egmont group, as well as federal law enforcement placement in countries all over the world to help stop the successful withdraw of cyber crime funds by criminal actors.

The FFKC is intended to be utilized as another potential avenue for US financial institutions to get victim funds returned. Normal bank procedures to recover fraudulent funds should also be conducted.

The FFKC can only be implemented if the fraudulent wire transfer meets the following criteria:

- the wire transfer is $50,000 or above;
- the wire transfer is international;
- a SWIFT recall notice has been initiated; and
- the wire transfer has occurred within the last 72 hours.

Any wire transfers that occur outside of these thresholds should still be reported to law enforcement but the FFKC cannot be utilized to return the fraudulent funds.

In order to initiate the FFKC, banks must provide the following information to their local FBI office.

Summary of the Incident:
Victim Name:
Victim Location (City, State):
Originating Bank Name:
Originating Bank Account Number:
Beneficiary Name:
Beneficiary Bank:
Beneficiary Account Number:
Beneficiary Bank Location (if available):
Intermediary Bank Name (if available):
SWIFT Number:
Date:
Amount of Transaction:
Additional Information (if available) - including "FFC"- For Further Credit; "FAV" – In Favor Of:

If the fraudulent funds are returned to the victim's account, the FBI requests that this information be passed back to their local field office contact.

TitleNews Online Archive

Hit by Wire Transfer Fraud? Use the Kill Chain Process

January 30, 2018

Criminals launder billions of dollars overseas through financial fraud schemes like wire transfer fraud, corporate account takeovers, business e-mail compromise scams and other financially motivated crimes.

The FBI offers a **Financial Fraud Kill Chain** (FFKC) process to help recover large international wire transfers stolen from the United States.

The FFKC is intended to be utilized as another potential avenue for U.S. financial institutions to get victim funds returned. Normal bank procedures to recover fraudulent funds should also be conducted.

The FFKC can only be implemented if the fraudulent wire transfer meets the following criteria:

- the wire transfer is $50,000 or above
- the wire transfer is international
- a SWIFT recall notice has been initiated
- the wire transfer has occurred within the last 72 hours.

Any wire transfers that occur outside of these thresholds should still be reported to **law enforcement** but the FFKC cannot be utilized to return the fraudulent funds.

Use these resources to help raise awareness about wire fraud:

- **wire fraud video**
- **wire fraud infographic**

*Contact ALTA at 202-296-3671 or **communications@alta.org**.*

American Land Title Association

Suffer a Data Breach? Here's Your First 24-Hour Checklist

Acting quickly and strategically following a data breach can help you regain your security, preserve evidence and protect your brand. According to Experian, it's important to collect, document and record as much information about the data breach and your response efforts, including conversations with law enforcement and legal counsel, as you can.

Once a breach is discovered, contact legal counsel for guidance on initiating these 10 steps:

1. Record the date and time when the breach was discovered, as well as the current date and time when response efforts begin, i.e. when someone on the response team is alerted to the breach.

2. Alert and activate everyone on the response team, including external resources, to begin executing your preparedness plan.

3. Secure the premises around the area where the data breach occurred to help preserve evidence.

4. Stop additional data loss. Take affected machines offline but do not turn them off or start probing into the computer until your forensics team arrives.

5. Document everything known thus far about the breach: Who discovered it, who reported it, to whom was it reported, who else knows about it, what type of breach occurred, what was stolen, how was it stolen, what systems are affected, what devices are missing, etc.

6. Interview those involved in discovering the breach and anyone else who may know about it. Document your investigation.

7. Review protocols regarding disseminating information about the breach for everyone involved in this early stage.

8. Assess priorities and risks based on what you know about the breach.

9. Bring in your forensics firm to begin an in-depth investigation.

10. Notify law enforcement, if needed, after consulting with legal counsel and upper management.

For more information on policies and procedures to protect non-public personal information, review ALTA's Title Insurance and Settlement Best Practices at www.alta.org/bestpractices.

CLAIM ALERT

FRAUDULENT EMAIL WIRING INSTRUCTIONS AND HOW TO MITIGATE YOUR RISKS

Connecticut Attorneys Title Insurance Company ("CATIC®") has experienced a number of recent claims regarding fraudulent wiring instructions.

The scams are similar:

- An Attorney is representing a person or entity in a real estate transaction;
- The Attorney either closes the real estate transaction with their own staff, or retains an Independent Paralegal ("IP");
- The fraudsters have infected computers of someone involved in the transaction, either the Attorney, the IP, the real estate agent, the seller's attorney, the buyer's attorney, the seller, the buyer or the broker;
- The virus allows the fraudsters to monitor email traffic between the parties;
- At some point, an email is sent by the fraudsters to the Attorney or IP with wiring instructions, which email address is similar to, if not indistinguishable from, the email addresses of the other parties in the transaction;
- The fraudsters then call the Attorney or IP to confirm receipt of the wire instructions;
- Believing that the confirmation has been made, the Attorney or IP then wires the funds per the wire instructions; and,
- Days later the fraudulent wiring instructions are discovered, but the wire cannot be reversed.

Result:
Besides the reputational harm, the scams result in the loss of proceeds, lawsuits are often filed, grievances may be filed, and personal liability may exist.

Mitigation Suggestions for Attorneys and IPs:

1. From the very start of any transaction, communicate and educate all parties on concerns and implement secure email practices;
2. If possible, enter into a "no payment change" rule with counsel on the other side of the real estate transaction prior to closing, that once the method and amounts of payments are set and agreed upon, no changes are tolerated without a substantial delay to reset and confirm that the proceeds have returned, and without a hold harmless agreement already in place;
3. Confirm any wire instructions received by calling your "known" contact (confirm and verify);
4. The fraudsters are aware that title insurance companies are requiring verbal confirmation of wires, and they are calling the Attorneys or IP themselves attempting to provide the required confirmation. Caller IDs even appear to be coming from a reputable source – but they are not. It is not enough to "receive" a confirming phone call. The Attorneys or IP should call their "known" contact to confirm and verify the wiring instructions;
5. Verify the telephone number from a reputable phone book, or search the business name via the internet;
6. Review your malpractice coverages and other insurance you may have with your insurance agents and carriers. Understand what your policies will cover, if anything, resulting from a fraudulent and/or wire transfer event. We have seen instances where, for example, the malpractice carriers have denied claims based upon the theory that the wire was a ministerial act and not the practice of law; and,
7. Purchase proper cyber and crime coverages with social engineering fraud/wire transfer protection included. Cyber and crime coverages, without the social engineering fraud/wire transfer protection, may not cover losses resulting from these transactions. Also read and understand the terms, provisions, limits, sub-limits and exclusions. There is a lot of variation.

Other General Computer Suggestions for Attorneys and IPs:
Email Spear Phishing is one method the fraudsters are using to gain access to computers. Email Spear Phishing is an email that appears to be from an individual or business that is known, but it is actually from a fraudster who wants credit card and bank account numbers, passwords, financial information and other data, or

OVER

CATIC'S CYBER SECURITY SOLUTIONS FORUM EXHIBITORS

ADNET Technologies is a technology consulting firm with offices in Farmington, CT and Albany, NY. Since 1991, our mission has been to connect people, process and technology to help our clients build a better business. For our clients, we strive to be the partner of choice; for our employees, the best place to work. Visit www.thinkADNET.com to meet our talented team and learn how ADNET guides clients to better ways to connect, collaborate and compete in a global market. http://www.thinkADNET.com

CATICPro, Inc. is a subsidiary of its parent holding company, CATIC Financial, Inc., and a sister company to CATIC®, New England's largest domestic and only Bar-Related® title insurance underwriter. CATICPro was formed in January 2003 to manage the business operations of the 1031 like-kind exchange services originally managed by CATIC back in the 1990s. Since then it has grown into a diversified service company, supporting the needs of the legal profession in the area of insurance, succession planning, and bonds. We pride ourselves on our high-quality services, focused customer service support and understanding of the legal community and its operations. http://www.caticpro.com

Connecticut Information Security is a full-service cyber security firm specializing in mitigating security risks, protecting networks, aligning organizations with security standards and educating workforce members on security-related topics and tools. We help protect organizations from security threats not only by determining their unique level of risk, but by providing expert insights based on best practice standards and proven remediation techniques. http://ctinfosec.com

Core Networks provides security engineers armed with the proper tools to help mitigate both personal data and fiscal loss. We are experts – whether you have a current security breach and need rapid incident response and network forensics; or are designing a web application and need to know common attack vectors and mitigation techniques. Core Networks focuses on providing organizations with complete cyber security services, solutions and consulting for New England area businesses. Across the region, we have the ability to do remote/multi-site engagements.
http://www.corenetworksinc.com

Direct iT, Inc. is a New England based IT services firm offering products and services for small businesses in Greater Boston, New Hampshire, Rhode Island, and the rest of New England. Cloud, compliance, and document management services are also available worldwide. Many of our customers are along the Route 128 technology corridor.
http://www.directitcorp.com

Foresite is a global service provider, delivering a range of managed security and consulting solutions designed to help our clients meet their information security and compliance objectives. In the face of increasingly persistent cyber-threats, Foresite's solutions empower organizations with vigilance and expertise to proactively identify, respond to, and remediate cyber-attacks and breaches where they occur. https://www.foresite.com

GuidePoint Security provides innovative and valuable cyber security solutions and expertise that enable organizations to successfully achieve their missions. By embracing new technologies, GuidePoint helps clients recognize threats, understand solutions, and mitigate risks present in their evolving IT environments. https://www.guidepointsecurity.com

CATIC
AGENT DRIVEN. INSURING RESULTS.

Call Us Toll Free at (800) 842-2216

CATIC PRO
PROFESSIONAL SOLUTIONS FOR YOUR BUSINESS

(860) 513-3131 | email@CATICPro.com

www.CATIC.com

www.CATICPro.com

CATIC's Cyber Security Solutions Forum Exhibitors

Palo Alto Networks is the next-generation security company maintaining trust in the digital age by helping tens of thousands of organizations worldwide prevent cyber breaches. With our deep cybersecurity expertise, commitment to innovation, and game-changing Next-Generation Security Platform, customers can confidently pursue a digital-first strategy and embark on new technology initiatives, such as cloud and mobility. This kind of thinking and know-how helps customer organizations grow their business and empower employees all while maintaining complete visibility and the control needed to protect their critical control systems and most valued data assets. https://www.paloaltonetworks.com

Wombat Security Technologies, headquartered in Pittsburgh, PA, provides information security awareness and training software to help organizations teach their employees secure behavior. Our Security Education Platform includes integrated knowledge assessments, a library of simulated attacks, and interactive training modules, which have been proven to reduce successful phishing attacks and malware infections by up to 90%. https://www.wombatsecurity.com

Zix is a leader in email security. Trusted by the nation's most influential institutions in healthcare, finance and government, Zix delivers a superior experience and easy-to-use solutions for email encryption and data loss prevention, advanced threat protection, archiving and bring your own device (BYOD) mobile security. Focusing on the protection of business communication, Zix enables its customers to better secure data and meet compliance needs. https://www.zixcorp.com