RE-ISAC Weekly Cybersecurity Report

Real Estate ISAC Information Sharing and Analysis Center

Serving the Commercial Facilities Sector

12 December 2017

TLP GREEN: Limited disclosure, restricted to the community. Sources may use **TLP GREEN** when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share **TLP GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP GREEN** information may not be released outside of the community.

YEAR IN REVIEW AND EMERGING THREATS

IN BRIEF: With one year coming to a close and a new year approaching, it is helpful to review the events of the previous year and make preparations for the events we anticipate in the near future.

KEY TAKEAWAYS & RECOMMENDATIONS:

- Several patterns emerged in 2017: Crime-as-a-Service, abuse of non-traditional IT devices to build botnets, increased targeting of cloud based architecture, and an evolution in social engineering to steal larger volumes of money and more information.
- The theft and exposure of confidential information increased in 2017. Many of these involved third-party providers.
- Greater awareness of insider threats led to the detection of more employee malfeasance and attempts at data theft in 2017.
- 2017 Also saw ongoing cyber compromise, theft, and disruption, as a result of geopolitical and economic events between nation-states. Sadly, the private sector is now specifically targeted, not just the military or government agencies.
- Many of the ongoing patterns will continue in to 2018, and there is a high likelihood that new tactics will emerge as individuals and organizations become more aware of cyber threats and take steps to prevent, detect, and mitigate crime.

YEAR IN REVIEW. For many years, cyber operators and incident responders took comfort in the assertion that while cyber events could result in serious economic impact or business disruption, they rarely resulted in harm to the health of safety of people. However, the proliferation of networked, wirelessly networked, even Internet connected devices in every aspect of life and business presented a broad attack surface for adversaries. **A few examples of direct or indirect impact emanate from the ransomware incidents that impacted hospitals, health records exchanges, and shipping and freight companies**. The health and welfare of people was impacted when emergency room operations were impacted by WannaCry and NotPetya ransomware strains. These both involved the resurgence of old self-propagation techniques. Additional blended risks came from the disruption of the card key system in a hotel, not the first such occurrence, and one that was mitigated by older components in the form of physical door locks which were not impacted by the disruption of the key-card system. Further blended threats were discovered in the proof of concept disclosures which demonstrated the danger to people of compromised robots used in various sectors. While system bugs can result in malfunctions that present risk to people,

A Blended Attack is deliberate, aggressive action that causes harm to both cyber and physical systems.

malicious software can, too. Furthermore, **the use or compromise of drones can result in harm to people and increased exploitation of vulnerabilities previously mitigated by air gaps that are now closed by the use of drones**.

Large scale robberies were carried out in 2017. Some involved extortion through the threat of denial of service, the threat of destructive malware, or the threat of releasing confidential information. Others exposed that nation states can also have financial motives as North Korea was attributed with financial theft that resulted from exploitation of the SWIFT messaging system. North Korea was also attributed to several large-scale ransomware or extortion campaigns.

The real winning tactics in 2017 stemmed from social engineering as opposed to technical sophistication. The Real Estate subsector was specifically targeted with wire fraud attempts leveraging email.

The Retail subsector was not forgotten as point-of-sale theft attempts persisted and payment information theft expanded to online retailers and those who provide platforms and payment processing services. The attack on Altos alone, affected more than 41 retailers. NotPetya also affected retailers. Payment information was not the only information exposed from retailers, Forever21 experienced the exposure of customer information due to a misconfigured Amazon S3 server containing a MongoDB instance. As usual, retailers continued to experience impersonation attempts causing customers to divulge credentials and other information to fraudsters.

Sports leagues, merchandisers, and athletes also experienced ongoing cyber incidents in 2017. The Sports Direct site experienced disruption from cyber actors and an operation known as FreeMilk impacted sports leagues in Europe. NFL free agents' information was exposed in another misconfigured cloud hosted database incident.

Hundreds of thousands of people were impacted by data stolen from the IRS FAFSA tool, a tool that helps parents and students applying for federal student aid auto populate tax information into the application forms. Information obtained from Equifax, universities such as Stanford, and W-2 Business email compromise scams put millions of additional people at risk for identity theft, tax fraud, and additional social engineering. Other opportunistic attempts at account takeovers in Gmail, Yahoo, and Microsoft's Office365 foreshadow additional attempts at account takeovers with financial institutions and other service providers as well.

Financial motives were not the only reasons for cyberattacks in 2017. Activism continues along with reputation management attempts, with several incidents relating to the **Entertainment and Media subsector**. North Korea used a cyber incident to persuade UK's Channel 4 to set aside a dramatic series about North Korea. BadRabbit targeted entertainment and media firms. Many production firms experienced the theft of data about new episodes and series as well as customer information. Extortionists attempted to realize payouts or release the stolen content publicly. One such actor, and Iranian national responsible for the theft and release of data from HBO was indicted by US federal authorities.

Hospitality and Lodging firms have been impacted by the breach of travel arrangement firms like Sabre while also working to mitigate rewards fraud and limit the impact of data breaches of other travel and transportation providers as well as point of sale compromises of collocated retail shops and restaurants. Even more importantly, **ransomware has disrupted hotel operations in one case preventing staff from providing key cards to guests checking in**. The proliferation of IoT devices provided additional attack surface for cyber exploitation. Many unprotected devices were recruited into botnets used for DDoS attacks (Persirai). Other botnets formed more recently (Reaper/IoTrooper) seemed to be tuned for data theft in addition to capabilities for disruption. More mischievous malware authors isolated vulnerable IoT devices for destructive activity (Brickerbot).

Many diverse services, applications, and businesses were disrupted by attempts to impede the global DNS system. A wide variety were impacted by misconfigurations of cloud based assets often configured and implemented by third parties. Furthermore, a flaw in Cloudflare's parsing engine resulted in the leakage of sensitive information about users of Cloudflare's services (Cloudbleed).

ANTICIPATED THREATS: Sadly, much of the activity observed in 2017 will continue into 2018. The proliferation of IoT devices that enable previously isolated sensors and operational technology to network with other systems, will continue to be targeted by adversaries of all types with a variety of motives. Some of this technology could result in harm to human health and safety while others may disrupt business or merely inconvenience users. The addition of unmanned vehicles on sidewalks, in buildings, in the air and on the roads, pose additional risk to resilience, confidentiality, and data integrity. These vehicles and devices have tremendous potential for positive outcomes, but also drastically change the nature of the network perimeter**. The risk from IoT proliferation applies to all types of commercial facilities.**

Non-traditional IT devices that are networked such as door locks, alarm systems, lightbulbs, dishwashers, toasters, refrigerators, coffee makers, energy meters, generators, surveillance cameras and associated DVRs, and badge access systems now require the same planning, monitoring, configuration, and maintenance as traditional IT assets. Traditional IT assets will continue to be exploited via the supply chain: hardware may be added, modified, or removed to achieve the desired adversary objectives. Furthermore, firmware vulnerabilities such as the AMT vulnerability in Intel processors (processors are found in all computing devices) will continue to occur. Better development and testing protocols in production phases will reduce these vulnerabilities, but those programs are difficult to implement. Whether the IT department is aware or not, these devices are becoming more common in all types of facilities and those who manage commercial real-estate, multifamily housing, or retail centers may contain these devices as implemented by tenants who lease space within the facility. Where systems could previously be air-gapped to reduce the attack surface, drones, and various wireless communications protocols have closed that gap. In the case of the Intel vulnerabilities the firmware used a proprietary protocol to communicate with remote resources.

Furthermore, **geopolitical and economic issues will result in increased targeting of the public and private sector by nation states. These threats will especially impact commercial facilities** as cyber or physical disruption of world events like the Olympic Games, the World Cup, the World Economic Forum, and various international meetings such as the G20, G8 and others serve as opportunities for messaging to reach a broad audience. The economic and geopolitical landscape will continue to result in terrorist attempts to harm people in large groups. The interconnectivity of vehicles like trucks, cars, drones may result in their use as weapons or delivery mechanisms for munitions or ordinance. Activists will continue to use website defacement, disruption, and other tactics to harm the reputation of those in opposition to their cause and to garner attention for their cause. Anonymous woke up again in 2017 to support the call for independence in Catalan in Spain**. The intended targets of such activities will range from media and entertainment companies, hospitality and lodging providers, arenas, concert halls, theaters, conference centers, and any events where people gather. Any buildings in the vicinity regardless of the ownership or occupancy could also become a target.** Sponsors and participants of such events are also frequently targeted for criminal and activist activity. According to a study by Distil Networks most real-estate websites are vulnerable to web scraping techniques.

Ongoing vulnerabilities in commonly used software, shared infrastructure, applications, firmware and operating systems will be exploited for espionage, extortion, reputational harm, identity theft or financial gain. Several strategies

that are working to discover and remediate vulnerabilities faster are third-party testing and certification regimes and responsible disclosure programs (also called bug bounty programs).

As long as social engineering is effective, adversaries will continue to use it. Real estate transactions will continue to be a high value target for financially motivated actors. **The 2017 tax season has already begun to see fraudulent tax returns filed. This activity will continue as it has been fueled by the data breaches of government agencies, credit reporting firms, health care institutions, educational institutions and more**. Residential data will also be continuously valuable to adversaries as **they need legitimate addresses to use to apply for credit cards and insecure mailboxes where they can receive fraudulently obtained payment cards and gift cards. The information released may also aid adversaries in impersonating insiders or customers in interactions with the enterprise and staff.**

Traditional IT schemes are still active. Malware designed to steal bank information, cashout ATMs**, infiltrate point-of-sale systems, and collect sensitive user activity for later use** will continue. In fact, **financially motivated actors continue to compromise email accounts of corporate personnel in order to use information observed to trade securities**. Leaks like the **Bermuda papers (similar to the Panama papers)** will continue to aid this activity and contribute to the loss of proprietary and sensitive corporate information.

Non-targeted and opportunistic activity such as the **delivery of crypto-currency mining tools via malvertising or watering hole techniques** will also continue and may increase as crypto-currencies rise in value and gain acceptance as currency. The migration to cloud based services and infrastructure will result in further targeting of cloud assets and personnel in cloud provider firms. Any misconfigurations, or lapses in monitoring or access management will likely be exploited by adversaries.

The outlook for 2018 is certainly more daunting than 2017, but dedication and proper prioritization of efforts through risk management will continue to help organizations reduce risk and navigate cyberspace with confidence.