OREGON CYBER TASK FORCE
SMALL BUSINESS THREAT ALERT

In 2015, Symantec Corporation found that 43% of all cyber attacks worldwide targeted small businesses of 250 or fewer employees.[1] Cyber criminals have learned that small businesses tend to have less robust security measures and are therefore easier to exploit compared to larger corporations. Nationwide Insurance in 2015 surveyed 500 small businesses and found that eight in ten did not have any cyber-attack response plan. Some of these businesses had already been victims of cyber intrusions.[2] With the growing cyber threats facing businesses today, it is the Oregon Cyber Task Force's goal to inform small businesses of current threats and how to reasonably protect themselves from these attacks.

PROMINENT EXISTING THREATS:

Business Email Compromise (CEO Fraud)

Business Email Compromise (BEC) involves cyber actors posing as business executives at companies that regularly perform wire transfers. After compromising the executive's email, the actor requests employees to perform wire transfers to the bad actor's account. The FBI Internet Crime Complaint Center (IC3) has reported over $3 billion of losses worldwide due to BEC. From January 2015 to June 2016, BEC has increased by 1,300%.

Ransomware

Ransomware is a form of malware that targets weaknesses in networks to deny the availability of critical data. Ransomware is frequently delivered through spear phishing e-mails to end users. When the victim organization determines they are no longer able to access their data, the cyber actor demands the payment of a ransom, at which time the actor will allegedly provide an avenue to the victim to regain access.

Point of Sale (PoS) Malware

Cyber criminals steal payment card data by remotely infecting PoS systems with malware without the need to physically access the cards or the devices used to process them. Consequently, cyber criminals can compromise PoS systems on a larger scale, increasing the number of potential victims.

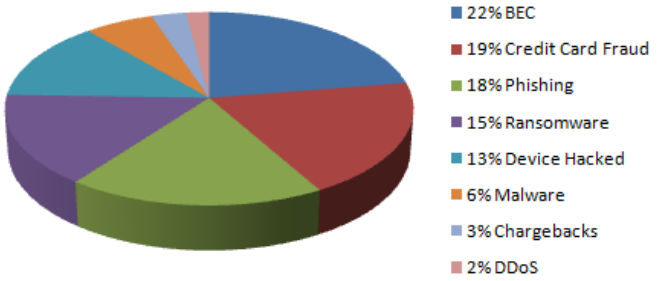
Insider Threat

An insider threat is a current or former employee who has or had authorized access to an organization's network and intentionally misuses that access to negatively affect the company. IC3 has recorded businesses losses from $5,000 to $3 million due to insider threats.

Internet Extortion

Internet extortion occurs when a cyber criminal hacks or threatens to hack a system and demands a ransom. Possible threats include a Distributed Denial of Service (DDoS) attack. One Oregon business reported that a hacker group threatened to perform a DDoS attack on their system if they did not pay a ransom of 50 bitcoin or roughly $30,000.

IC3 Complaints Received From Oregon Businesses in June 2016



Oregon Cyber Task Force || 9109 NE Cascades Parkway, Portland, Oregon 97220 || (503) 460-8000 || octf.pd@ic.fbi.gov

Prevention Considerations:

- Implement an awareness and training program. Because end users are targeted, employees and individuals should be made aware of the threats.
- Patch operating systems, software, and firmware on devices every couple weeks. This process may be made easier through a centralized patch management system.
- Ensure anti-virus and anti-malware solutions are set to automatically update every day and that regular scans are conducted weekly.
- Manage the use of privileged accounts. Implement the principle of least privilege: no users should be assigned administrative access unless absolutely needed.
- Configure access controls, including file, directory, and network share permissions, with least privilege in mind.
- Disable macro scripts from office files transmitted via e-mail.
- Implement application whitelisting; only allow systems to execute programs known and permitted by security policy.

Business Continuity Considerations:

- Back up data regularly, and regularly verify the integrity of those backups.
- Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Examples might be securing backups in the cloud or physically storing offline.
- Backups are critical in ransomware; if you are infected, this may be the best way to recover your data.

The Ransom:

The FBI does not support paying a ransom to the adversary. Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with an escape route after paying a ransom. Paying a ransom emboldens the adversary to target other organizations for profit, and provides for lucrative environment for other criminals to become involved. While the FBI does not support paying a ransom, there is an understanding that when businesses are faced with an inability to function, business owners will evaluate all options to protect their business, employees, and customers.

If you believe your company has been a victim of a cyber intrusion, contact the Oregon Cyber Task Force or other law enforcement agency.

RESOURCES:

- **Cyber Task Force (CTF)**

www.fbi.gov/contact-us/field

The FBI Cyber Division has established CTFs in each of the FBI's 56 field offices. CTFs are staffed with cybersecurity professionals who respond to cyber incidents, conduct victim-based investigations, and collect malware signatures and other actionable intelligence. FBI Headquarters works directly with CTFs to build a strategic picture of cyber threats, attribute attacks, plan operations, and disseminate timely threat information to victims and private partners.

- **Internet Crime Complaint Center (IC3)**

www.ic3.gov

IC3 provides the public with an online reporting mechanism for suspected internet-facilitated crime, including intellectual property theft and online fraud. Complaints are processed and sent to relevant U.S. Government agencies for follow-up action and intelligence collection.

1, 2 www.foxbusiness.com/features/2016/04/27/cyber-attacks-on-small-business-on-rise.html