What is the Ransomware Landscape?
What is Ransomware?

- Ransomware is typically a low end malware
- It is typically part of a larger attack infection chain
  - Key is to block the initial loading agent from entering into the environment
- Purpose is to lock system access to critical files by encrypting the data
- Tends to spread as a worm after initial infection causing greater risk to organizations
- Ransomware has historically been associated to Nation State attackers
  - Motivations: Funding, Incident Response monitoring, Infrastructure Damage
- Sharp decline over the last 2 yrs but in past 8 months on a major upswing
- Examples: GandCrab and Sodinoknobi (email) Ryuk and SamSam (not mail) but in many cases the entry compromise was mail
Hacking is a Business

proofpoint.
Defenders don’t focus on people, Attackers do

IT Security Spending
- Network: 62%
- Endpoint: 18%
- Email: 8%
- Web: 12%

Attack Vectors
- 93% of all breaches are attacks targeting people, 96% via email

Source: Gartner (2017 forecast)
Source: 2018 Verizon DBIR
Seehotel Jaegerwirt

- Beautiful 4 STAR hotel
- Can pay C$634 per night
- Locked out key function and removed the capability of the hotel to open doors to rooms and make new keys
- Paid Bitcoin 2,367 C$
- It happened 4 times……
- Went back to manual keys 😊
Question which would be worse for an org? Ransomware or a standard data breach?
Ransomware is dead they said…..????

- 22 attacks 1st half of yr and now more than one a week
- In what is a first for Louisiana, its governor has declared a state of emergency after three school systems in the state were hit with cyberattacks.
- Syracuse ransomware operators increase their demands as victims miss payment deadlines-July 2019
- Lake City, Florida fires its IT director after paying hackers $460K in ransom-June 2019
- Key Biscayne, and Riviera Beach-600k paid out

*Ransomware is fundamentally a denial of service attack, and when services are denied to the public, it becomes a significant issue for government.*
The complexity we face—Multi-staged attacks

1. Ransomware infection launched by USER opening a malicious attachment from an email
2. Attachment contained Upatre downloader
3. Downloader infected the user with GameOver Zeus
   - GameOver Zeus a stealer trojan banking/other data
4. Then Upatre would download Ryuk
5. Ryuk encrypted files and demanded a ransom

*Most common point of failure is the USER*
Cred Phishing as the Trigger

- Increase in phishing of enterprise cloud services
  - dropbox, box, onedrive, salesforce...
  - O365 phishing is a major issue

- PDFs containing links

- Not limited to email
  - SMS, Social, etc.

- Often the first stage of a larger attack
  - After infiltration, remain persistent
  - Recon for Impostor phishing
Grandcrab calling it quits in Q2?

All the good things come to an end.

For the year of working with us, people have earned more than $2 billion, we have become a nominal name in the field of the underground in the direction of crypto-fiber. Earnings with us per week averaged $2,500,000. We personally earned more than 150 million dollars per year. We successfully cashed this money and legalized it in various spheres of white business both in real life and on the Internet. We were glad to work with you. But, as it is written above, all good things come to an end.

We are leaving for a well-deserved retirement. We have proven that by doing evil deeds, retribution does not come. We proved that in a year you can earn money for a lifetime. We have proved that it is possible to become number one not in our own words, but in recognition of other people.

In this regard, we:
1. Stop the set of adverts;
2. We ask the adverts to suspend the flows;
3. Within 20 days from this date, we ask adverts to monetize their bots by any means;
4. Victims - if you buy, now. Then your data no one will recover. Keys will be deleted.

That's all. The topic will be deleted in a month. Thank you all for the work.
Cyber Fear Ransomware

You have to send money by the end of the workday, if the workday is over and people start leaving the building explosive will detonate.
This was just a year ago this occurred.

---

U.S. » Bomb threats emailed to multiple locations across the country

From:  
Sent: Thursday, December 13, 2018 12:05 PM  
To:  
Subject: -- SPAM -- My device is inside your building

Hello. I write you to inform you that my man carried the explosive device (lead azide) into the building where your company is conducted. It was built according to my guide. It can be hidden anywhere because of its small size, it is impossible to destroy the structure of the building by my explosive device, but if it explodes there will be many wounded people.

My mercenary is controlling the situation around the building. If he notices any suspicious behavior, panic or emergency he will power the bomb.

I can withdraw my recruited person if you make a transfer. $20'000 is the price for your life and business. Pay it to me in BTC and I assure that I have to withdraw my recruited person and the bomb won't detonate. But do not try to cheat - my assurance will become valid only after 3 confirms in blockchain network.

Here is my Bitcoin address:

You have to solve problems with the transfer by the end of the workday, if you are late with the money the device will explode.

Nothing personal this is just a business, if you don't transfer me the bitcoins and the bomb detonates, next time other commercial enterprises will pay me a lot more, because it isn't a one-time action.

For my safety, I will no longer enter this email account. I check my address every 35 min and if I see the payment I will give the command to my mercenary to get away.

If an explosion occurred and the authorities notice this email- We arent a terrorist society and dont take liability for acts of terrorism in other buildings.
Why is Ransomware returning?

• The Bitcoin Money Trail
• More distribution channels
  – Botnet network
  – Polymorphic malware
  – Malicious URL’s
• Better Targets
• Cryptocurrency growth and lack of controls
• No repercussions
Baltimore

- Baltimore’s “lack of investment in cybersecurity when it had already fallen victim to a similar attack” was not good for the city’s credit, wrote Moody’s analyst Nisha Rajan.

- After spending more than $10 million (hearing up to 18 million) to restore its computer networks, the city had planned paying $835,000 to cover itself in case of future attacks
Impact Response

• Mayors won’t pay……lets see how that goes
• IF they don’t pay, they get fired. IF they pay, they get fired.
• Must have FULL backup capabilities
  – This is much easier at a local level based on the smaller size

If they don’t pay, guess who is next…States and Utilities

#1 reason ransomware is distributed is email and #1 reason for infection is social engineering
To Pay or not to Pay-That is the Question…..

- Paying a ransom does not guarantee an organization will regain access to their data
- Some victims who paid the demand were targeted again by cyber actors
  - (they tell their friends)
- After paying the originally demanded ransom, some victims were asked to pay more
- Having Insurance pick up the tab may cause more harm than good
- Paying could inadvertently encourage the bad behavior
Recommendations
How to Prepare

- Backup and secure those backups
- Update and Patch
- Implement an awareness and training program
- Teach users how they need to respond if they get infected
- Enable strong Email Security to prevent phishing emails
- Authenticate inbound email
- Privilege account management
- Disable RDP if at all possible
- Create proper segmentation
  - Question are we connecting and automating for speed for the sake of speed or is there a real “critical value”
During the Storm

How to react

- Call law enforcement
- Disconnect from network- create break point to segment sites
- Disconnect Backup from the network too
- Change all online account passwords and network passwords
- Triage depth of infiltration
- Orchestrate Response
- Restore
  - Don’t assume free tools for encryption will work (they typically don’t)
After the Storm Clears

Shoring up for the next Attack

• Clean up
• Post-mortem review
• Assess User Awareness and response
• Educate on what to look for and what to do if happens
• Invest in Modern Defenses
• Focus on specifics of what the actor did, ransomware may just be a side effect
The Move to the Cloud - It’s Here…..

ANYTIME, ANYWHERE, ANY DEVICE ACCESS

Email | Collaborate | Share Files
Download & Upload Files | Use external facing portals

Network | Device | Client

Accidental Sharing of Data
Compromised Credentials
Compliance Risks

NEW RISKS

Compromised Credentials
Layers of the Cloud

• For Revenue and Customer Communication
• Information sharing
• For Data Storage
• For Leveraging 3rd Parties to do more
• Public access cloud
Reward of Cloud

• Reduction in cost
  - Physical costs
  - Reduction in Operational and Management upkeep
  - Refocus employees on more useful tasks that relate to the “actual business”
  - Allow required IT components to be patched and protected in a more timely fashion
  - Leveraging greater computing power resources
  - Leveraging tools that allow businesses to do more
  - Use third party resources as needed

• Leveraging Other resources
  - Expertise
  - Or speed to market
Risk of Cloud

- Data managed by 3rd party
- All customers in one place
  - Target for evil doers is greater
- Trust of vendors is needed
- Ramifications of Breach
- Who has access to data?
Biggest trend: Rising Wave of O365 Attacks

• Significant increase in organized attacks on O365 accounts
• Allows for INTERNAL Social manipulation
• Increasing as the Cloud move becomes larger
• Variety of techniques
  - Brute-force appears to be the most common initial vector
  - Use botnets to scale across many O365 tenants
  - Password reuse from mega-breaches
  - Phishing
• Managed Cloud - centralized data for attacker
• Rapidly developing different techniques

proofpoint
Real World Impact of Compromised Accounts

CEO’s O365 Account Compromised

Attackers Access Email, Calendar

Wait for Supplier Meeting

Email CFO Requesting Wire

From: Real CEO
To: Real CFO
Stuck in this meeting. Can you send a wire to acct 5551212? It’s the last thing we need to close the deal.
Bypass MFA and breach cloud accounts

- Study looked at over 100,000 logins
- 72% of tenants were targeted at least once by threat actors
- 40% of tenants had at least one compromised account in their environment
- 15 out of every 10,000 active user-accounts were successfully breached by attackers
- Attacker method was INTERNAL Phishing
- Changed forward rules or delegations to maintain persistence
- Leveraged IMAP to bypass MFA
Cloud Risks: Accidental Sharing of Sensitive Info

**PFPT Findings**

**Files Shared Publicly**
- 23,000

**Files Shared w/ Entire Organization**
- 300,000

**Files Shared w/ Personal Accounts**
- 8,000 by 2.5% of users

**Gaming and Hospitality – Office 365 Customer**

- VP of Finance shared One Drive directory publicly
- HR shared termination letters with entire organization
- Sr Engineer shared passwords w/ personal account

**Proofpoint Cloud App Security Broker**

- Identified sensitive data, owner and sharing settings
- Detected folders/files shared publicly or with entire organization
- Notified user/admin & suggested “reduce permissions”
Partner Network Exposure

• This is a **HUGE** risk
• Fast developing organizations leveraging 3\textsuperscript{rd} party partners to do more with less resources
• Partners are connected to us (VPN), Directly, Authentication
• Segmented out
• For how long are they connected? what is the specific need?
• Why doesn’t it have the same level of security as the internet?
What to look for in a provider

• Physical Security
• Redundancy
• Recovery Plan
• Access control
• Data Storage
• 3rd party provider partner augmentation
• How much can you control VS the vendor
• Can you see the controls and security steps that are taken
• Listen closely to the way the vendor talks about security vs their product
• How do they hire?
• Maintenance plan and outages
• Leverage social media crowdsourcing for details on outages and recovery
• Be concerned if you ask for security details and they DON’T push back some
Leveraging Cloud with Customers
Protecting Brands from Domain Fraud

Domain Monitoring – For every well-known brand-owned domain on the internet, there are hundreds or thousands of suspicious lookalikes domains potentially defrauding their customers

- No barrier to entry for domain registrations
- Variety of fraudulent techniques to imitate a brand
Protecting Brands from Social Phishing scams

@_CocoaDream: @Ask_WellsFargo what number do I call if I want to speak to someone about my account?
@WF_Helpline: @_CocoaDream Sign in at <> . You can set up a new one and move to the next page.
Proofpoint gives you protection and visibility for your greatest security risk—your people.

We provide the most effective security and compliance solutions to protect people on every channel including email, the web, the cloud, and social media.
Final Thoughts

• When designing, assume you will get breached, how do you minimize impact
• Watch how vendors share information and interact
  – Vendors who do cloud need to have it as part of their culture
• Don’t do it just because everyone else does
• Try not to tie Apps to Cloud data
  – App organizations typically do not have strong controls
• Your users are the entry point to cloud failure so you must train them on how to use the cloud correctly
• Ensure vendors have strong monitoring and are not waiting for you to tell them there are problems