



# Security At-a-glance

Feb 2020 Webinar



- Uplevel status update
- Security layer overview
- Breakdown of:
  - Threats from the outside
  - Threats from the inside
  - Responses to exploits
- Protect from multiple angles

# Uplevel Update

- Introduced the ***world's first*** cloud-controlled Active Directory Server in a firewall!
- Third party partnerships
- 100% growth in partner and customer base in 2019
- Expanded to address customers with up to 100 employees



# The State Of Security

Hacks used to be ...  
To make a point



Now they are done to make 💰

- Steal & sell your data to someone else
- Lock up and sell your data back to you

# Recent Events



- 23 Texas Counties were hit with Ransomware
  - Through a third-party vendor!
- \$2.5 Million Ransom demand

But First  
Let's Take A Step Back....



# Multi-faceted Attack Landscape

## Progression of Attacks

1. Attackers get into the network
  - Unsolicited outside attacks
  - Attacks from the inside via compromised machines
2. Phone home to command-and-control server
3. Move around the network to find insecure unprotected devices
4. Find critical data on the network
5. Watch traffic for passwords and access to additional resources
- 6a. Exfiltrate data back to mother servers to sell or publish
- 6b. Or encrypt data and demand ransom.



# Outside -> In Attacks

# Attacks From The Outside

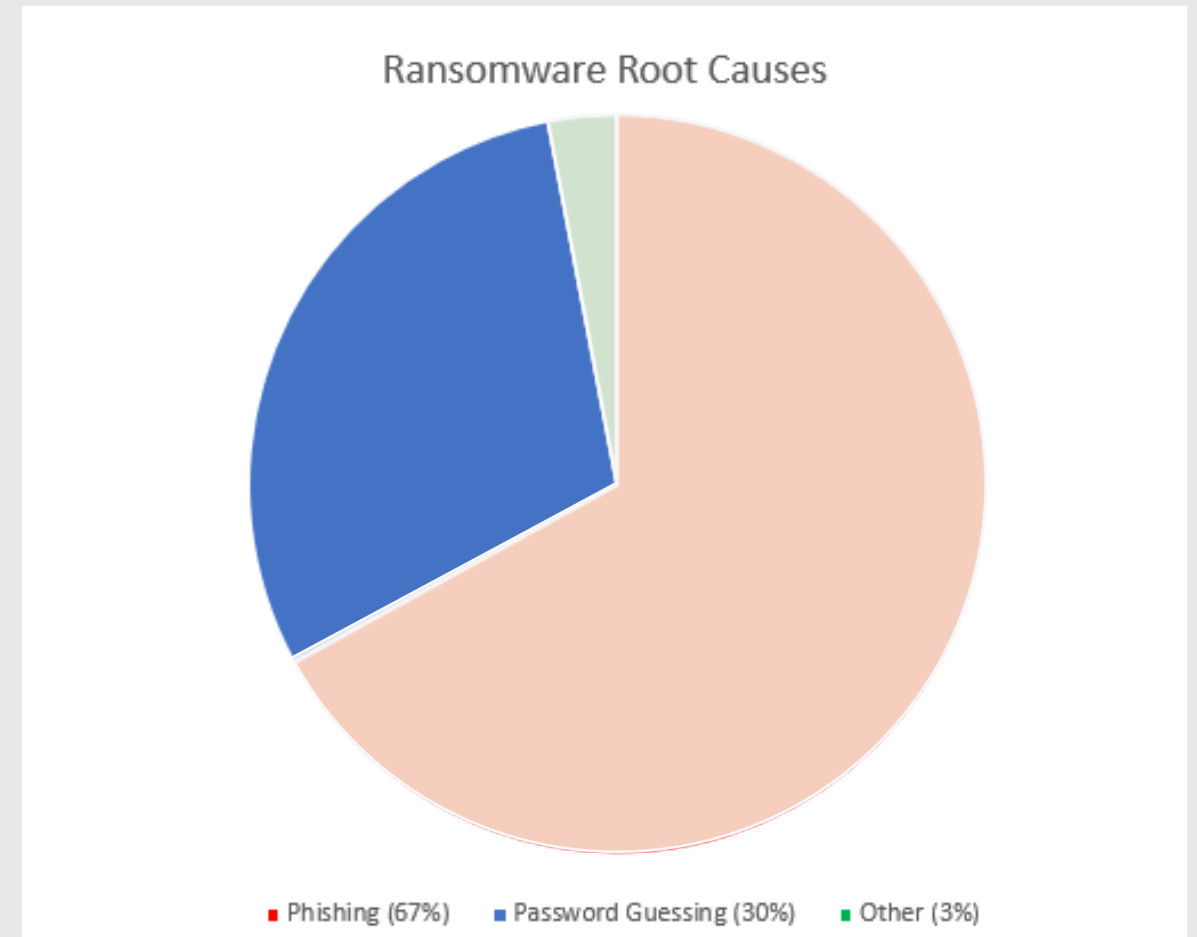
- Over 3,000 attacks per day on average to each firewall
  - No firewall? Immediate access!
- Attacks primarily originating from:
  - United States
  - China
  - Russia
  - Iran
- Cloud servers also at risk

*“Hackers are going after servers that haven’t been set up correctly, allowing them to view sensitive information and extract it with minimal effort” - Wall Street Journal*

<https://www.wsj.com/articles/human-error-often-the-culprit-in-cloud-data-breaches-11566898203>

# Outside -> In Intrusion

- Getting into the network with
  - Out of date firewalls/routers
  - Unused/unrestricted firewall holes
  - Unpatched VPN servers
  - Brute force of RDP passwords
  - Unrestricted third-party vendors



KnowBe4's "Now That Ransomware Has Gone Nuclear, How You Can Avoid Becoming the Next Victim?" Webinar

# Outside Attacks

- Getting into the network with
  - Out of date firewalls/routers
  - Unused/unrestricted firewall holes
  - Unpatched VPN servers
  - Brute force of RDP passwords
  - Unrestricted third party vendors

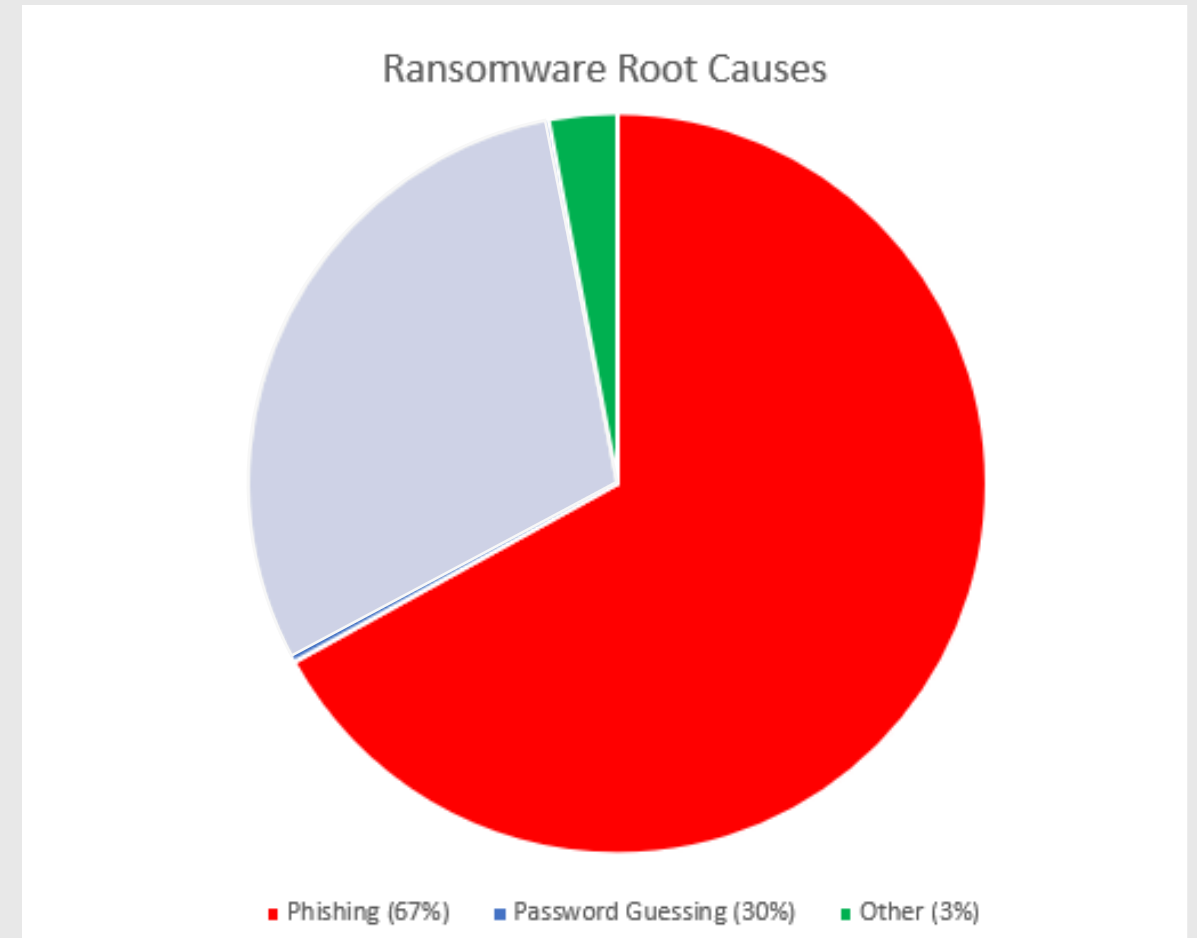
## Protect by:

- Keep all infrastructure up to date
- Block *all* unsolicited traffic, including pings
- Close all firewall ports – use VPNs
- Limit any open ports by source IP/DNS
- Use geoblocking to shut off known attack sources
- Restrict third party access to premises equipment
- Ensure cloud infrastructure is secured

# Inside -> out Attacks

# Inside -> Out Intrusion

- Getting into the network with
  - Phishing emails
  - Malicious advertisements
  - Bad website traffic
  - Unsecure device/applications with unlimited access
  - Out of date client machines
  - Compromised VMs



KnowBe4's "Now That Ransomware Has Gone Nuclear, How You Can Avoid Becoming the Next Victim?" Webinar

# Protection Against Inside->Out

- Getting into the network with
  - Phishing emails
  - Malicious advertisements
  - Bad website traffic
  - Unsecure device/applications with unlimited access
  - Out of date client machines
  - Compromised VMs

## Protect by:

- Ensure all machines have antivirus and antimalware kept up-to-date
- DNS filter all web accesses
- Geoblock accidental phishing ads
- Geoblock malware from phoning home to control server
- Restrict insecure application access
- Segregate insecure IoT devices
- Inspect traffic for malicious content
- Keep device firmware updated

# Once Hackers Are In





Access to hackers = Access to the affected machine

Without additional protection they can:

- Attack other machines
- Replicate data over to their servers
- Encrypt data or delete files

# Protect Customers

- Only allow known devices/users
  - Domain Management
- Ensure all devices kept updated
- Restrict access to resources
  - NAS partitions
  - Internal firewall rules
- Segregate insecure devices with VLANs
  - IoT devices
- Restrict hackers from moving data abroad



**RANSOM!**

# Protecting Customers

- From hackers wanting to...
  - Sell their data to others
  - Sell their data back to them
- Lines of defense
  - Regularly scan the network
  - Stay updated on current events and tactics
  - Regularly monitor backups
  - Regularly evaluate credentials
  - Monitor network for anomalous events & traffic

- If Tragedy Strikes?
  - Have a recovery plan!

# How Does Uplevel Help??

- Keep the LAN side easy to configure
  - Automatically ensures correct and secure configurations
  - No inadvertent openings
- Keep infrastructure up to date
  - Automatic updates to signatures
  - Periodic automatic firmware updates
- Keep customers Secure
  - Variety of security options: Geoblocking, Content Filtering, IDS/IPS, etc.

# Attacks Are Only The Symptom!

The disease is how they got in!

- Repeat attacks often occur
- Paying a ransom now doesn't prevent future attacks

Blocking threats, remediating any that get in, and constant vigilance are the keys



# A Bit Of Housekeeping

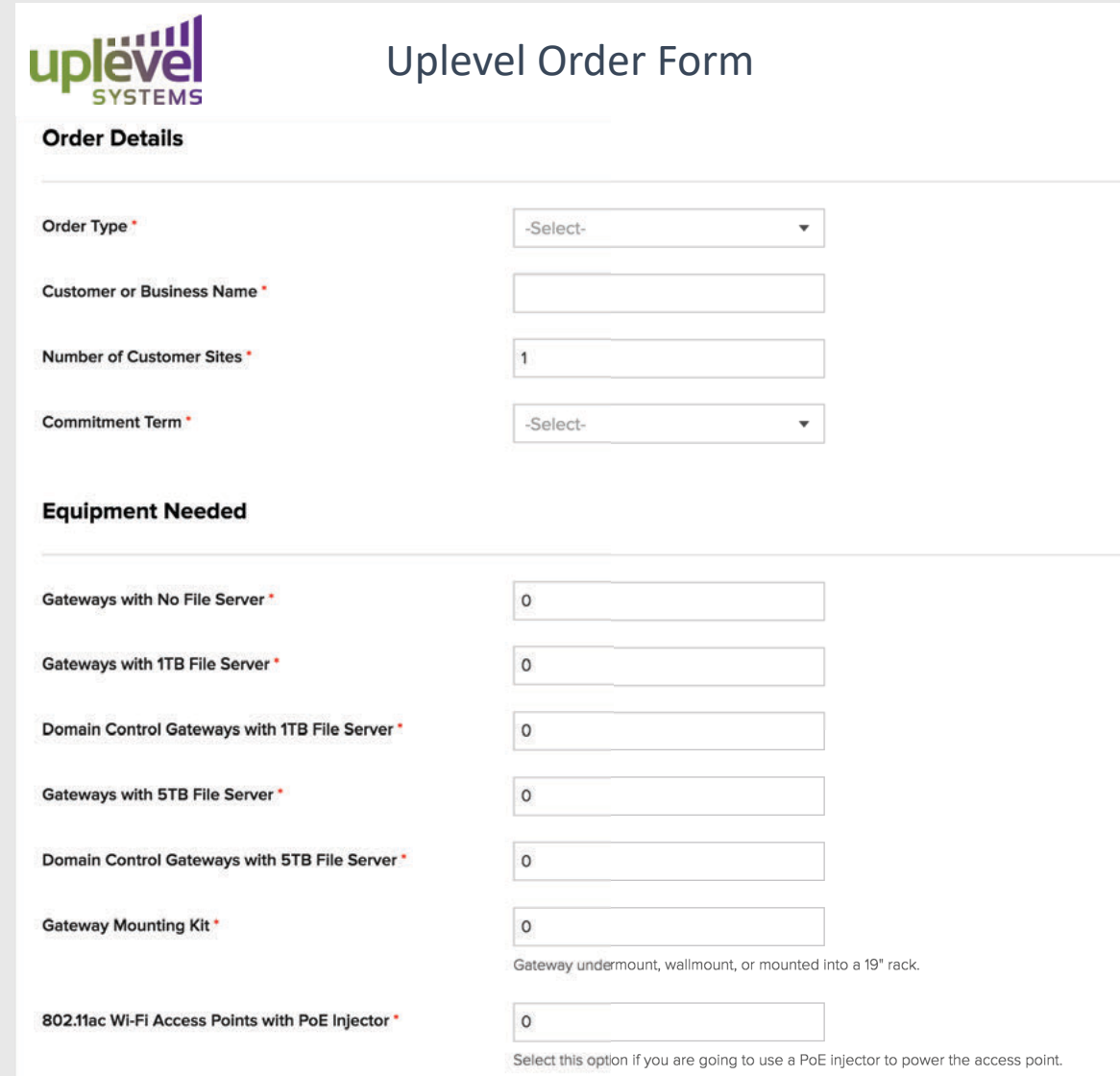
# New Order Placing Links

Want to test out the new AD system?

<https://zfrmz.com/J9D6OKdXwP3JRtkjcQft>

Looking to order a system?

[www.uplevelsystems.com/order](http://www.uplevelsystems.com/order)



**Uplevel Order Form**

**Order Details**

Order Type *	<input type="text" value="-Select-"/>
Customer or Business Name *	<input type="text"/>
Number of Customer Sites *	<input type="text" value="1"/>
Commitment Term *	<input type="text" value="-Select-"/>

**Equipment Needed**

Gateways with No File Server *	<input type="text" value="0"/>
Gateways with 1TB File Server *	<input type="text" value="0"/>
Domain Control Gateways with 1TB File Server *	<input type="text" value="0"/>
Gateways with 5TB File Server *	<input type="text" value="0"/>
Domain Control Gateways with 5TB File Server *	<input type="text" value="0"/>
Gateway Mounting Kit *	<input type="text" value="0"/>
<small>Gateway undermount, wallmount, or mounted into a 19" rack.</small>	
802.11ac Wi-Fi Access Points with PoE Injector *	<input type="text" value="0"/>
<small>Select this option if you are going to use a PoE injector to power the access point.</small>	



# Questions?

[Support@uplevelsystems.com](mailto:Support@uplevelsystems.com)  
[www.uplevelsystems.com/order](http://www.uplevelsystems.com/order)