Tales Of True Tech Crimes: Ripped From The Headlines

K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

About Brian Tankersley @BFTCPA

CPA, CITP, CGMA with three decades of Accounting and Technology business experience, including public accounting, industry, consulting, media, and education.

- ***Director, Strategic Relationships***, K2 Enterprises (k2e.com) (2005-present)
  - Delivered presentations in 48 US states, Canada, and Bermuda.
- **Freelance Writer** for accounting industry media outlets such as AccountingWeb and CPA Practice Advisor (2015-present)
- ***Podcast Host, The Technology Lab for CPA Practice Advisor**, 2020-present*
- ***Author**, 2014-2021 CPA Firm Operations and Technology Survey*
- ***Director, Strategic Relationships / Instructor***, Yaeger CPA Review (2017-present)
- ***Publisher***, CPATechBlog.com (2004-present)
- ***Technology Editor***, The CPA Practice Advisor (CPAPracAdvisor.com) (2010-2014)
- Selected nine times as a "Top 25 Thought Leader in Public Accounting Technology" by *The CPA Practice Advisor*.
- 2012 and 2009 Outstanding Discussion Leader Award, *TN Society of CPAs*
- Author of numerous articles and have direct consulting experience with and for numerous organizations such as software vendors and CPA Firms.
- brian@k2e.com // @BFTCPA // +1(865) 684-4707

CPA CITP Certified Information Technology Professional

K2 Enterprises Copyright 2022, K2 Enterprises, LLC

Session Description

We're all familiar with the headlines describing how criminals use new and creative approaches to commit their crimes. But what you may not know is that these same criminal elements also target accounting professionals. Unfortunately, accountants are one of the most targeted groups on the Internet!

In this session, you will learn how high-profile failures occurred due to control malfunctions. In turn, hackers gained full reign over entire networks that contained sensitive information such as financial data stored online. Attend this session so you can be more effective at preventing crimes such as theft, malware, ransomware, phishing, and hacking.

K2 Enterprises Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Learning Objectives

- List at least three major security incidents reported in the headlines in the last year and explain at least one primary control design or operation flaws that allowed the hack to occur
- Select the correct definitions from a list of standard security terms such as attack surface, vulnerability, exploit, social engineering, phishing, malware, heuristics, biometrics, and multi-factor authentication
- List at least three best practices learned because of reviewing the incidents cited in the case studies

Copyright 2022, K2 Enterprises, LLC

Overview Of Presentation

- Phishing Enabled Ransomware Attack
- Botnet Infects 40,000 Routers Then Used for Cybercrime
- E-mail Accounts Compromised, Mined for Data
- Ransomware Payments Up Significantly in 2021
- Ontario Brewery Business E-mail Compromise
- SMS Interception Using Business Texting Tools
- Miscellaneous Privacy and Productivity Perils
  - Antivirus and cryptomining
  - Everyone wants your earnings data

Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

"Inside a Ransomware Hit at Nordic Choice Hotels",
WSJ Pro, January 12, 2022

PHISHING ENABLED RANSOMWARE ATTACK

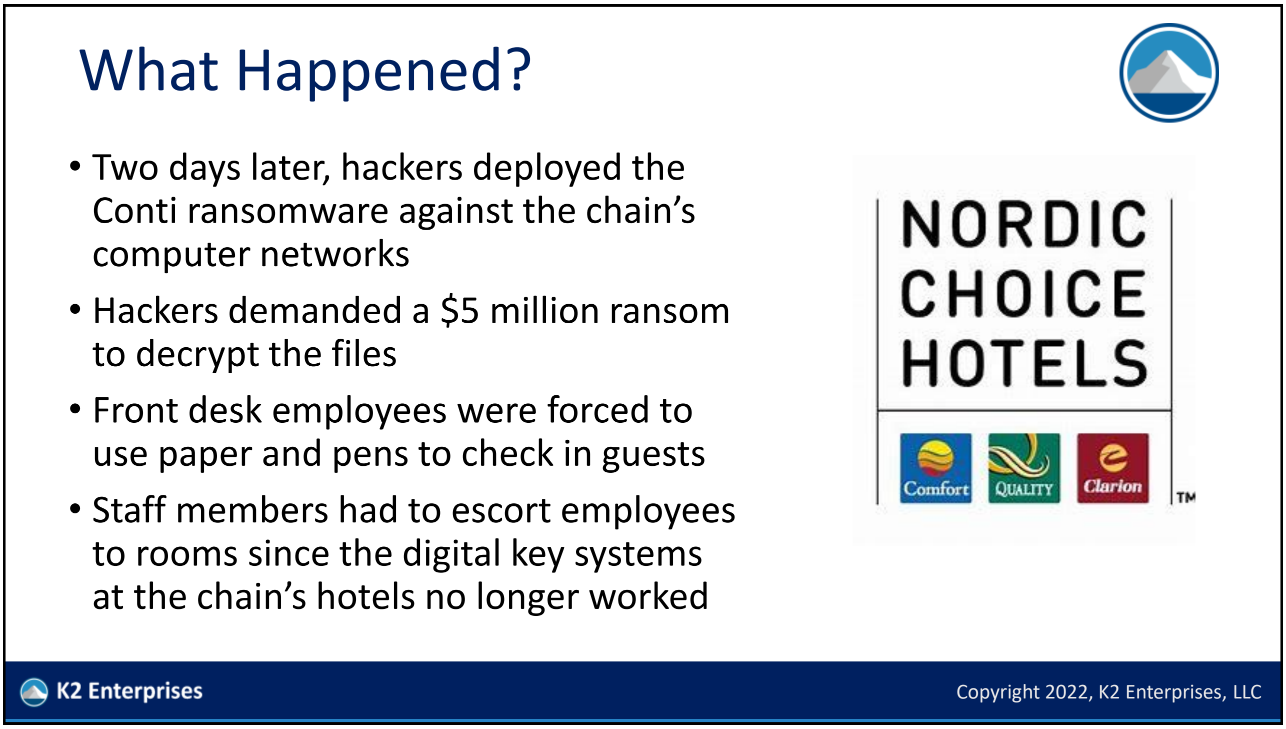
Copyright 2022, K2 Enterprises, LLC

What Happened?

- Nordic Choice Hotels is hotel operator of hotels branded by Choice Hotels, Inc. (Comfort, Quality, Clarion) in Norway, Sweden, Denmark, Finland and Lithuania
- Sometime on November 29, 2021, a tour operator e-mailed a Nordic Choice Hotels employee
- The employee clicked on a malicious website link
- This mistake made it possible for hackers to disable antivirus apps, download data, and install apps

Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

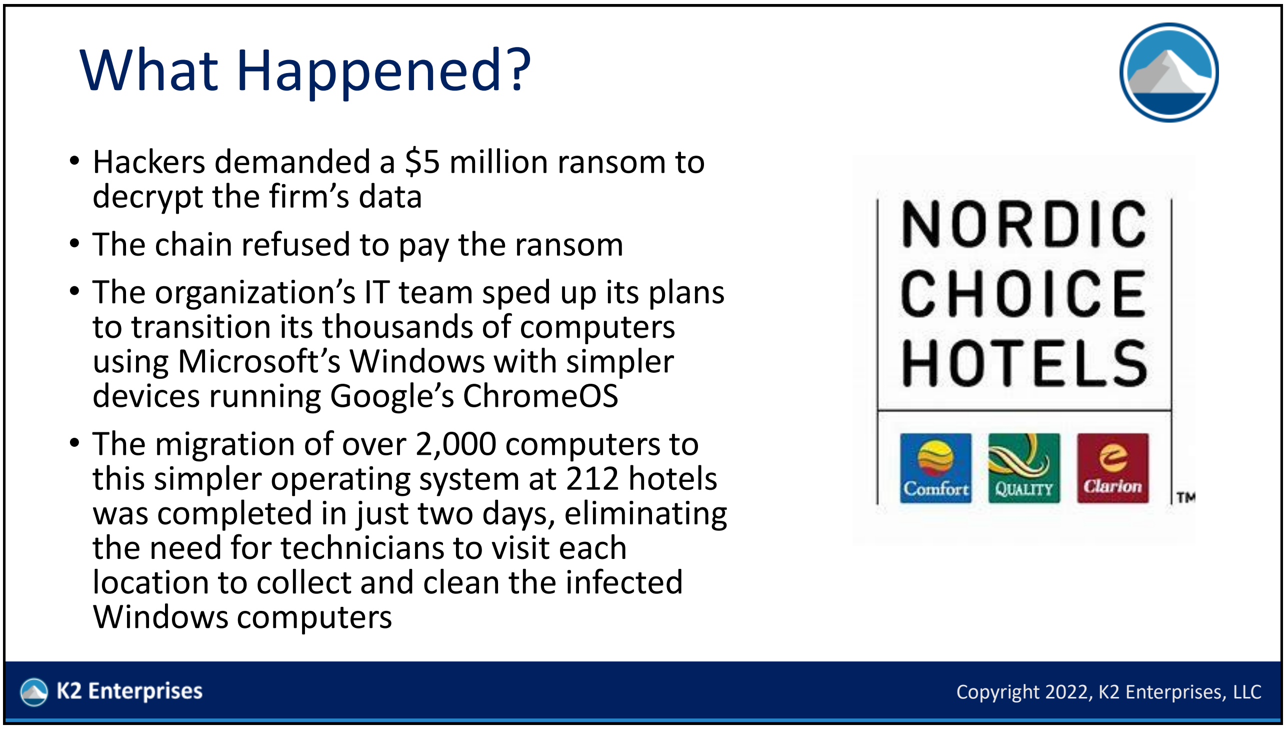


What Happened?

- Two days later, hackers deployed the Conti ransomware against the chain's computer networks
- Hackers demanded a $5 million ransom to decrypt the files
- Front desk employees were forced to use paper and pens to check in guests
- Staff members had to escort employees to rooms since the digital key systems at the chain's hotels no longer worked

K2 Enterprises

Copyright 2022, K2 Enterprises, LLC



What Happened?

- Hackers demanded a $5 million ransom to decrypt the firm's data
- The chain refused to pay the ransom
- The organization's IT team sped up its plans to transition its thousands of computers using Microsoft's Windows with simpler devices running Google's ChromeOS
- The migration of over 2,000 computers to this simpler operating system at 212 hotels was completed in just two days, eliminating the need for technicians to visit each location to collect and clean the infected Windows computers

K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

What Happened?

- Five weeks later, the chain reported that there were still some fixes needed to address glitches in heating, music, and other systems at some properties
- Hackers posted personal data about employees to the dark web, including government ID data and bank info
- Thankfully, hackers were unable to access data on the chain's guests
- NCH has created staff training courses on how to recognize fraudulent e-mails, but only after the damage was done

NORDIC
CHOICE
HOTELS

Comfort QUALITY Clarion ™

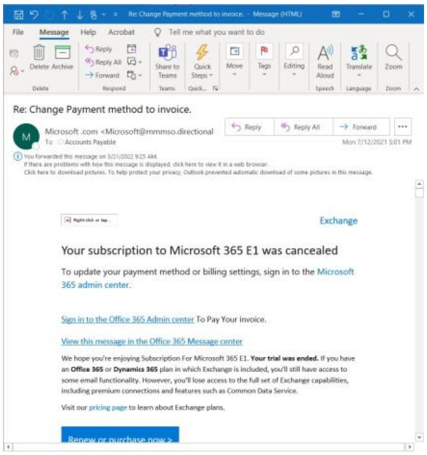
"Microsoft the No. 1 Most-Spoofed Brand in Phishing Attacks",
Dark Reading, March 16, 2022

DARK
Reading

MICROSOFT IS TOP PHISHING BRAND

Spear Phishing: Still Significant

- According to the March 2022 publication, “Spear Phishing: Top Threats and Trends” by Barracuda Networks
  - 51% of social engineering hack attacks are phishing
  - Microsoft is the most impersonated brand, used in 57% of phishing attacks
  - An average small business with <100 employees will receive 350% MORE social engineering attacks than an employee of a large enterprise



Re: Change Payment method to invoice.

Microsoft .com <Microsoft@mmmso.directional
To Accounts Payable
Mon 7/12/2021 5:01 PM

You forwarded this message on 3/21/2022 9:25 AM.
If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Your subscription to Microsoft 365 E1 was cancealed

To update your payment method or billing settings, sign in to the Microsoft 365 admin center.

Sign in to the Office 365 Admin center To Pay Your invoice.

View this message in the Office 365 Message center

We hope you're enjoying Subscription For Microsoft 365 E1. **Your trial was ended.** If you have an **Office 365** or **Dynamics 365** plan in which Exchange is included, you'll still have access to some email functionality. However, you'll lose access to the full set of Exchange capabilities, including premium connections and features such as Common Data Service.

Visit our pricing page to learn about Exchange plans.

One of literally hundreds of MS365/O365 phishing e-mails received by the author

Copyright 2022, K2 Enterprises, LLC

Spear Phishing: Still Significant

- According to the March 2022 publication, “Spear Phishing: Top Threats and Trends” by Barracuda Networks
  - Cybercriminals compromised ~500,000 MS 365 accounts - just in 2021
  - 1 in 5 organizations had an account compromised in 2021
  - 1/3 of malicious logins came from Nigeria
  - Cybercriminals sent out 3,000,000 messages from 12,000 compromised accounts
  - Conversation hijacking grew by 270% in 2021

Spear Phishing:
Top Threats and Trends

Vol. 7 March 2022

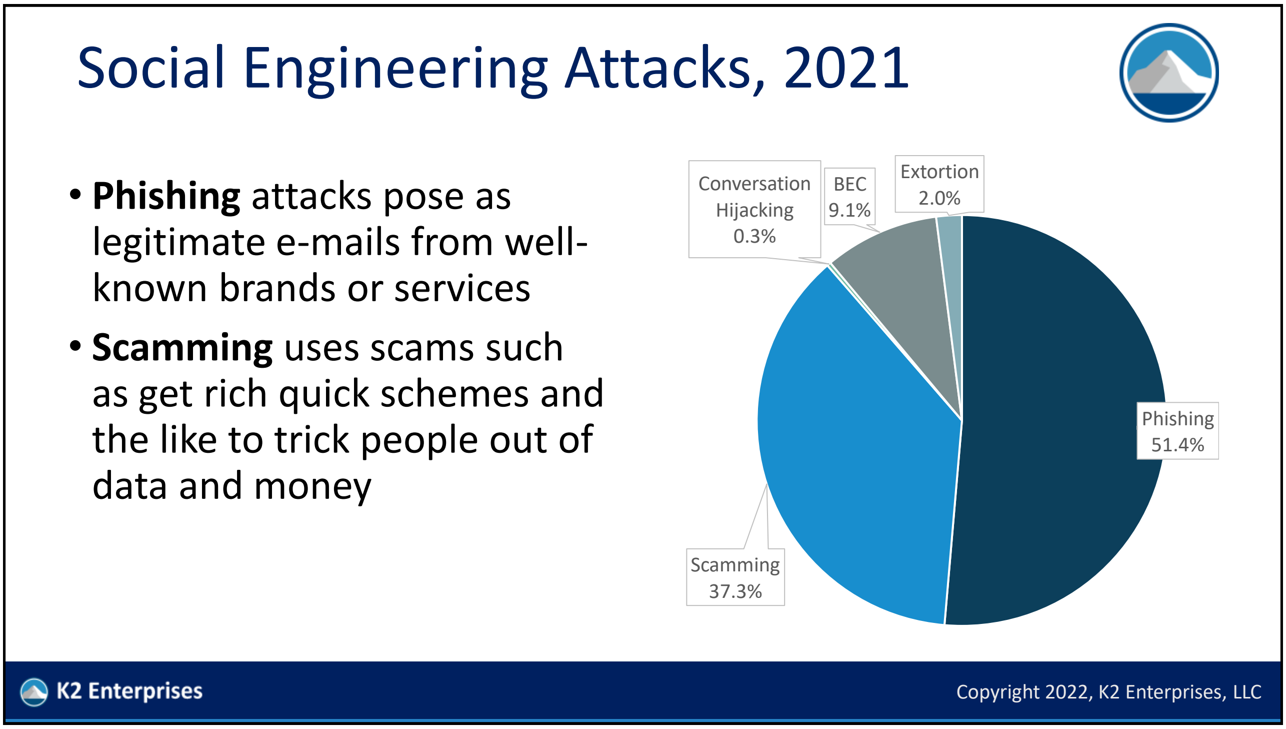
Key findings on the latest social engineering tactics and the growing complexity of attacks

Cybercriminals are constantly refining their tactics and making their attacks more complicated and difficult to detect. In this in-depth report, Barracuda researchers share their insights on the most recent trends in social engineering and the new methods attackers are using to trick their victims.»

Barracuda
Your journey, secured.

Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

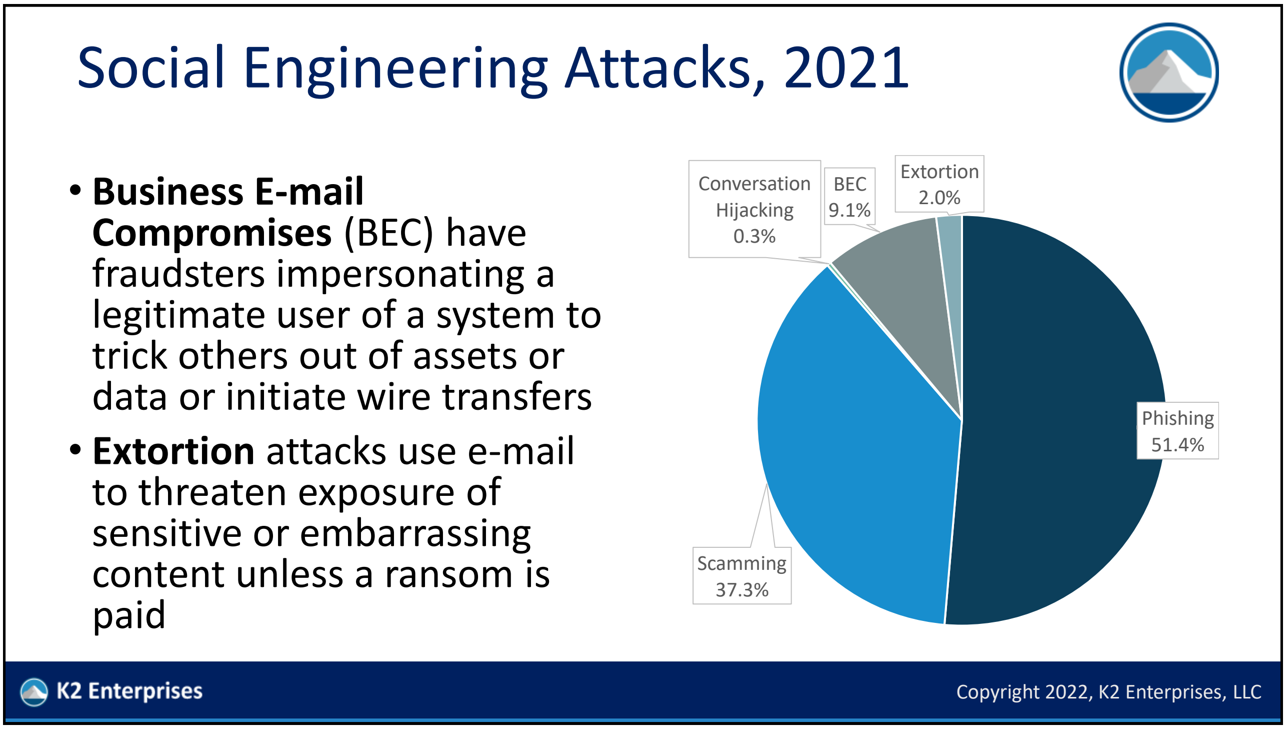


Social Engineering Attacks, 2021

- **Phishing** attacks pose as legitimate e-mails from well-known brands or services
- **Scamming** uses scams such as get rich quick schemes and the like to trick people out of data and money

K2 Enterprises

Copyright 2022, K2 Enterprises, LLC



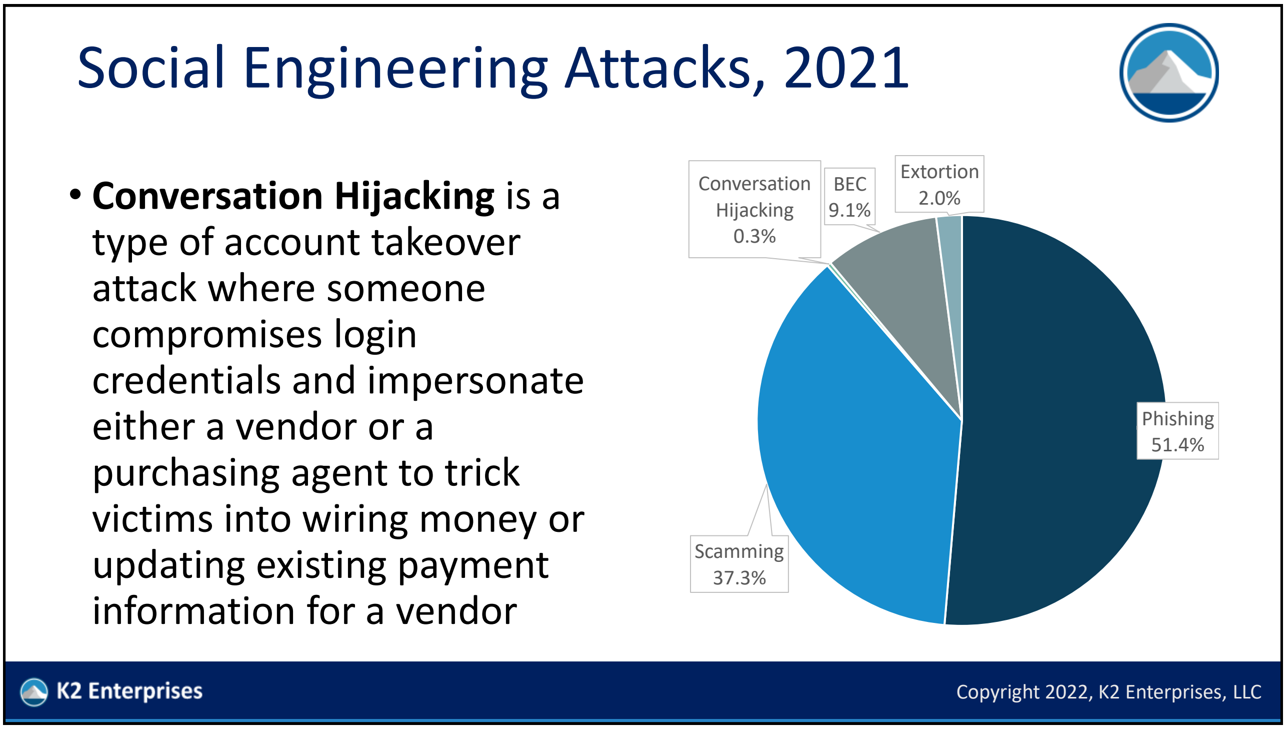
Social Engineering Attacks, 2021

- **Business E-mail Compromises** (BEC) have fraudsters impersonating a legitimate user of a system to trick others out of assets or data or initiate wire transfers
- **Extortion** attacks use e-mail to threaten exposure of sensitive or embarrassing content unless a ransom is paid

K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

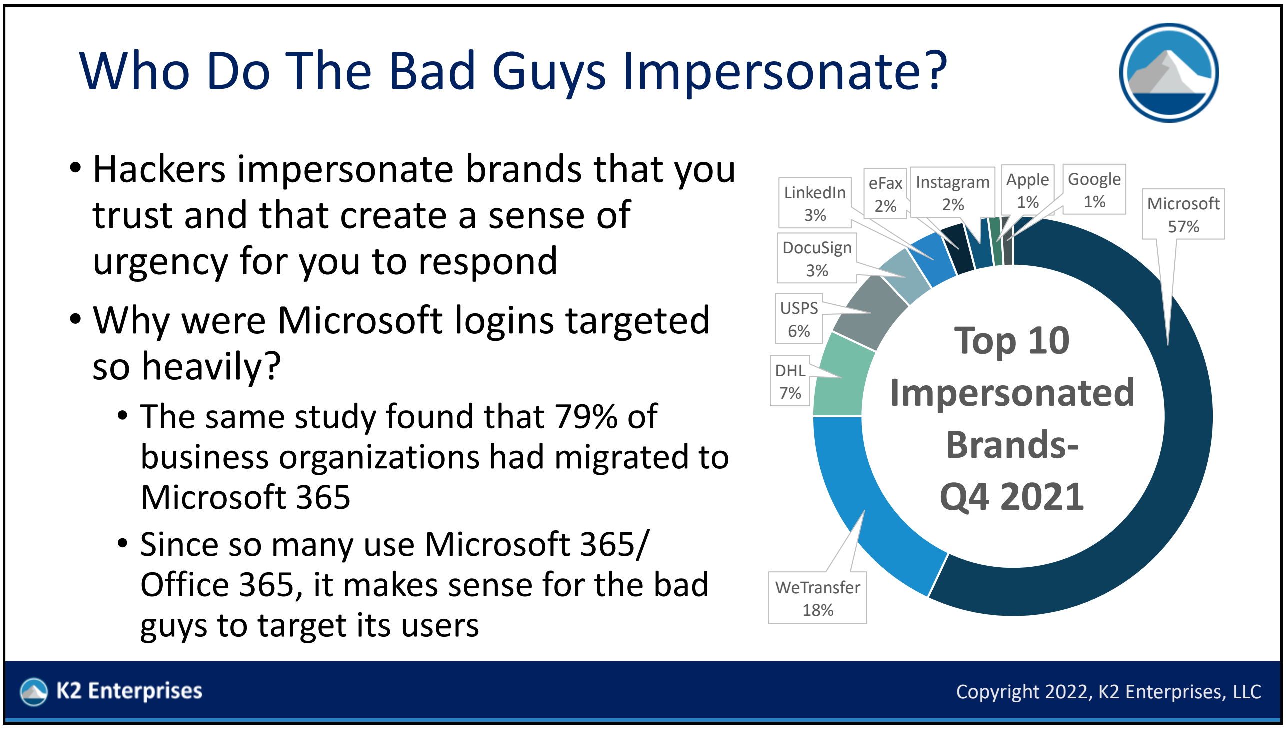
Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.



Social Engineering Attacks, 2021

- **Conversation Hijacking** is a type of account takeover attack where someone compromises login credentials and impersonate either a vendor or a purchasing agent to trick victims into wiring money or updating existing payment information for a vendor

Copyright 2022, K2 Enterprises, LLC

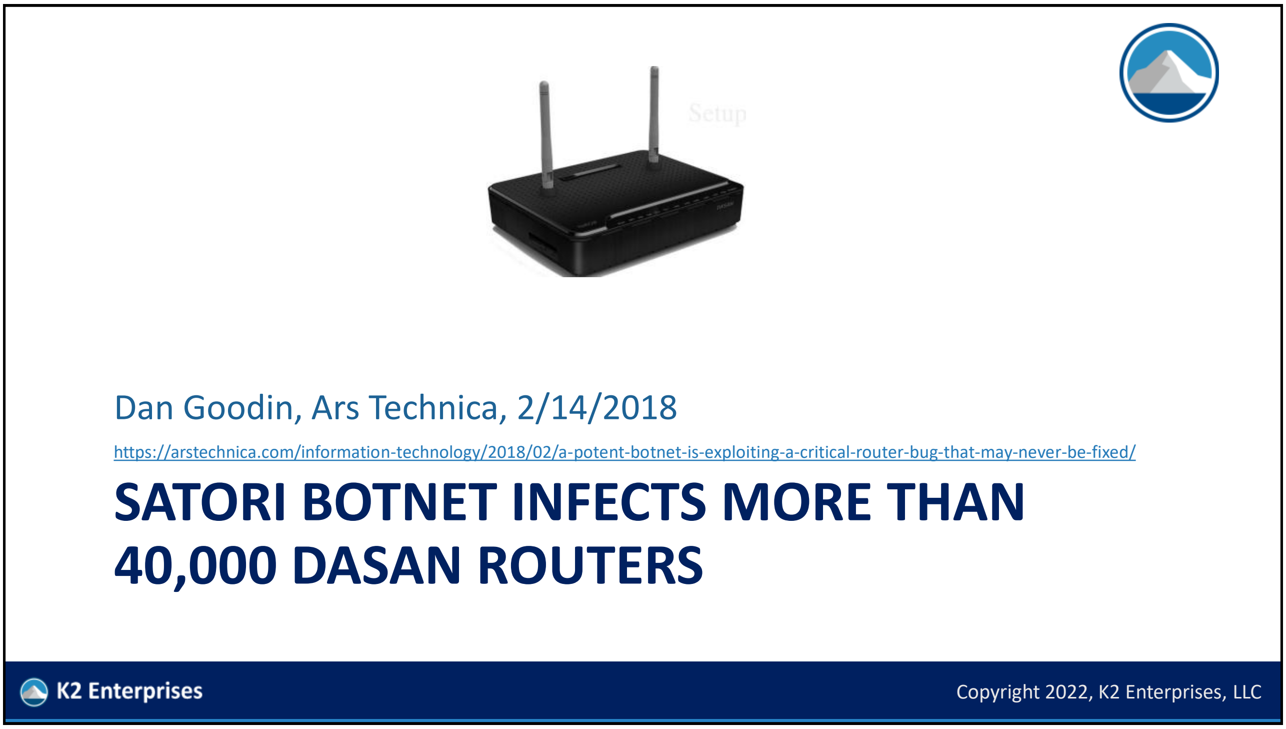


Who Do The Bad Guys Impersonate?

- Hackers impersonate brands that you trust and that create a sense of urgency for you to respond
- Why were Microsoft logins targeted so heavily?
  - The same study found that 79% of business organizations had migrated to Microsoft 365
  - Since so many use Microsoft 365/ Office 365, it makes sense for the bad guys to target its users

Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.



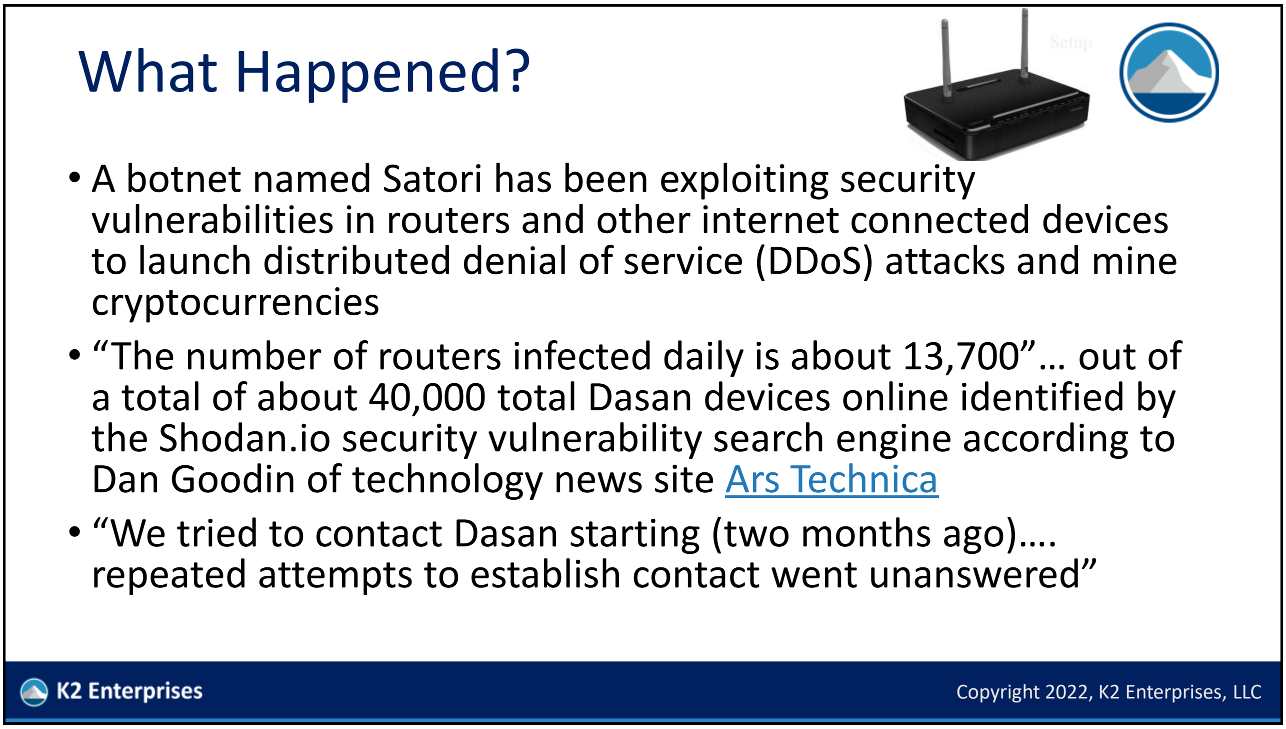
Dan Goodin, Ars Technica, 2/14/2018

https://arstechnica.com/information-technology/2018/02/a-potent-botnet-is-exploiting-a-critical-router-bug-that-may-never-be-fixed/

SATORI BOTNET INFECTS MORE THAN 40,000 DASAN ROUTERS

K2 Enterprises

Copyright 2022, K2 Enterprises, LLC



What Happened?

- A botnet named Satori has been exploiting security vulnerabilities in routers and other internet connected devices to launch distributed denial of service (DDoS) attacks and mine cryptocurrencies
- “The number of routers infected daily is about 13,700”… out of a total of about 40,000 total Dasan devices online identified by the Shodan.io security vulnerability search engine according to Dan Goodin of technology news site Ars Technica
- “We tried to contact Dasan starting (two months ago)…. repeated attempts to establish contact went unanswered”

K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

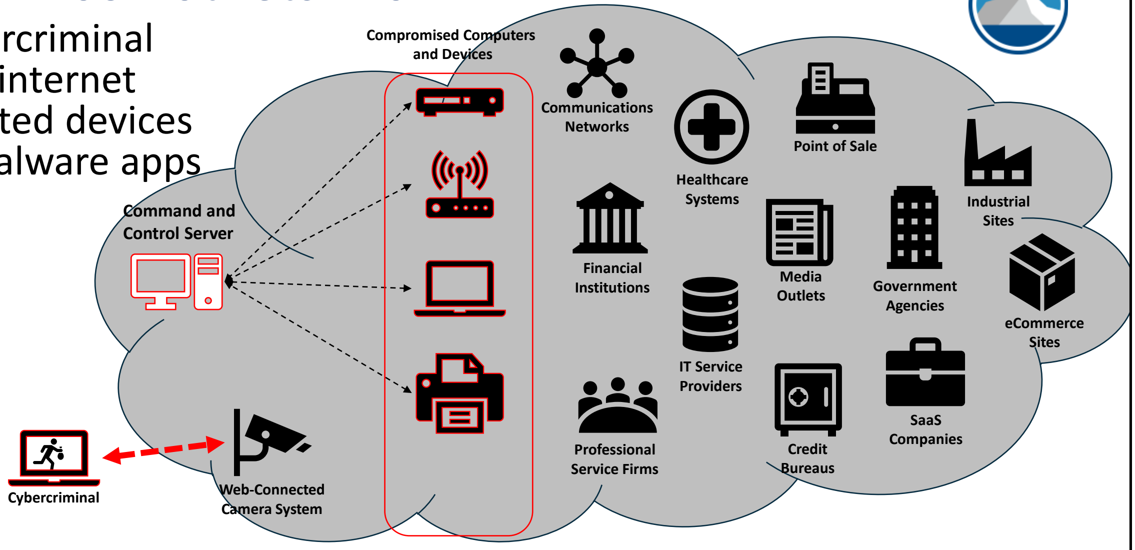
The Satori Botnet

- Is based on the Mirai malware which compromised internet-connected devices like routers and digital video recorders who had not changed the default passwords
- This kind of botnet is often used to extort money from big websites in exchange for not shutting them down
- Exploits bugs in embedded firmware to take control of internet exposed devices
- Home grade devices are often poorly configured and rarely receive the timely security updates necessary to keep them safe from hackers

K2 Enterprises
Copyright 2022, K2 Enterprises, LLC

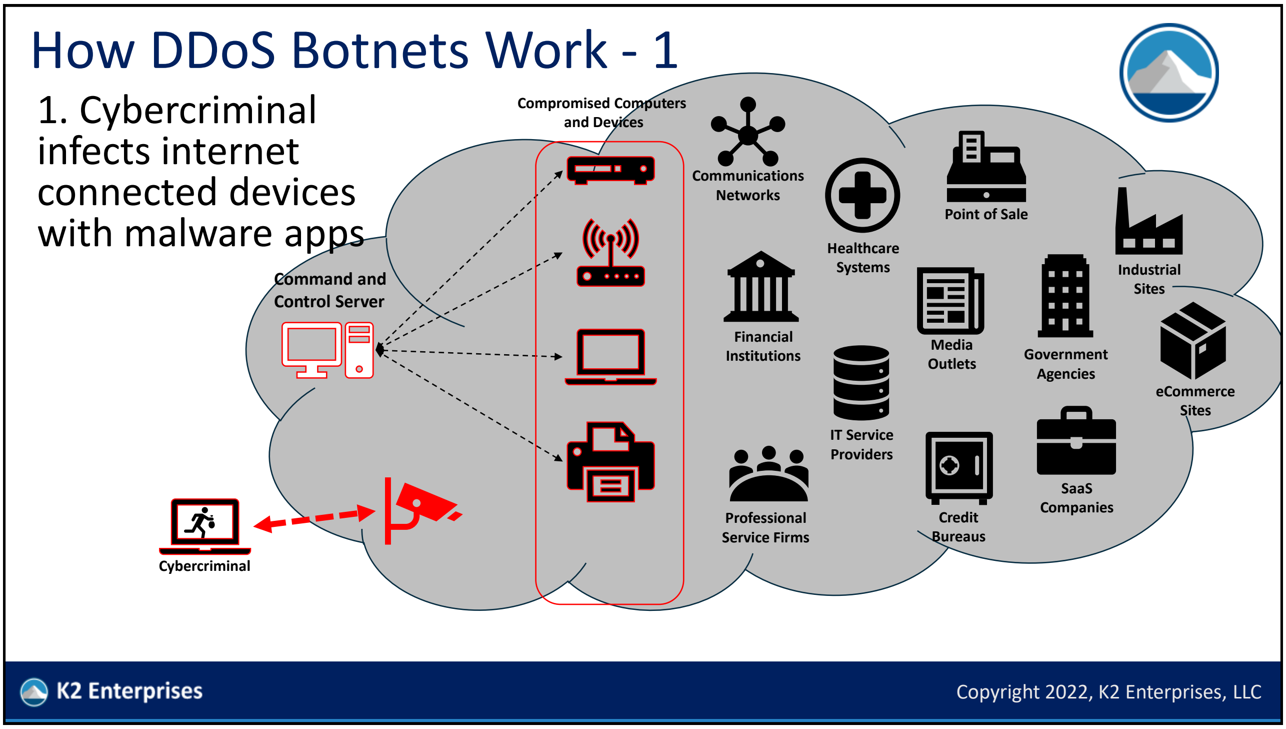
How DDoS Botnets Work - 1

1. Cybercriminal infects internet connected devices with malware apps



K2 Enterprises
Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

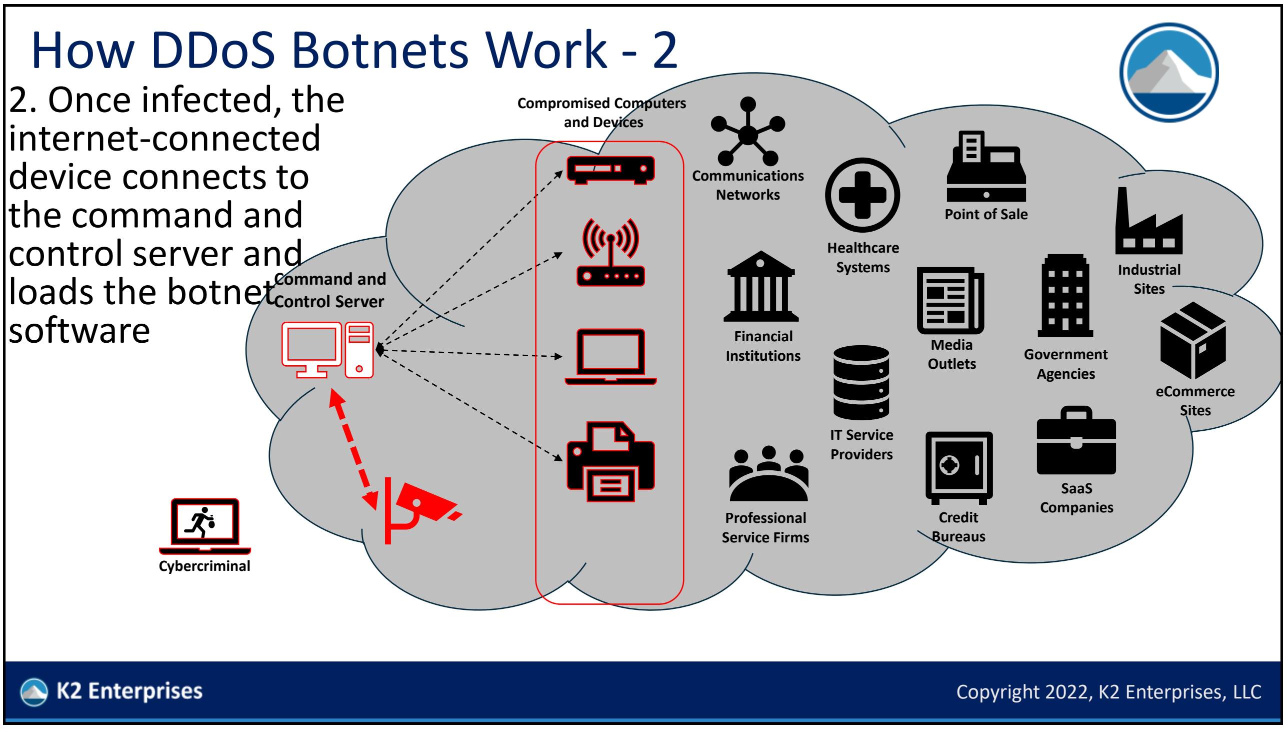


How DDoS Botnets Work - 1

1. Cybercriminal infects internet connected devices with malware apps

K2 Enterprises

Copyright 2022, K2 Enterprises, LLC



How DDoS Botnets Work - 2

2. Once infected, the internet-connected device connects to the command and control server and loads the botnet software

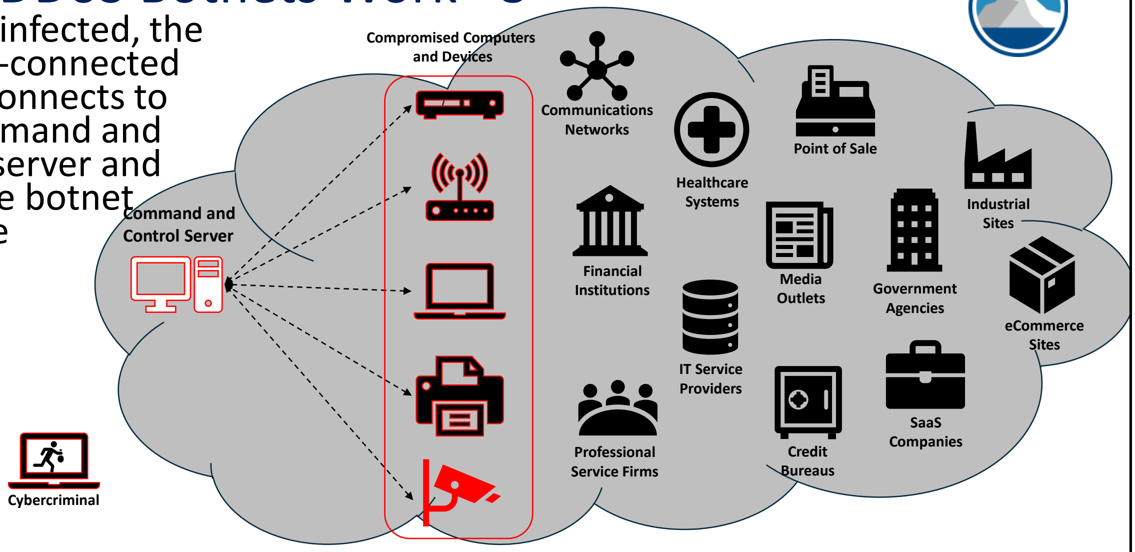
K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

How DDoS Botnets Work - 3

3. Once infected, the internet-connected device connects to the command and control server and loads the botnet software

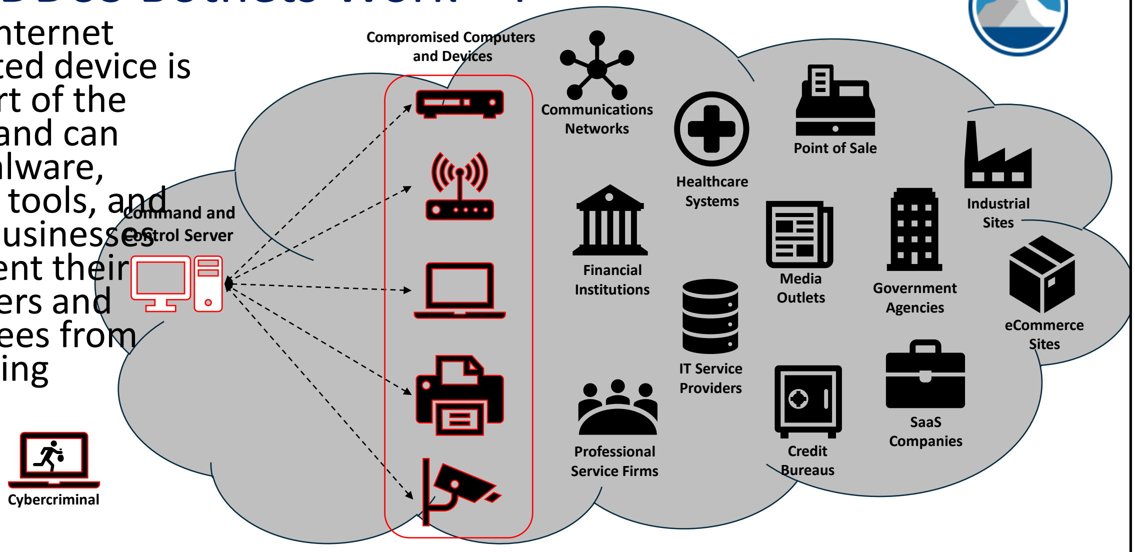


K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

How DDoS Botnets Work - 4

4. The internet connected device is now part of the botnet and can load malware, hacking tools, and target businesses to prevent their customers and employees from interacting



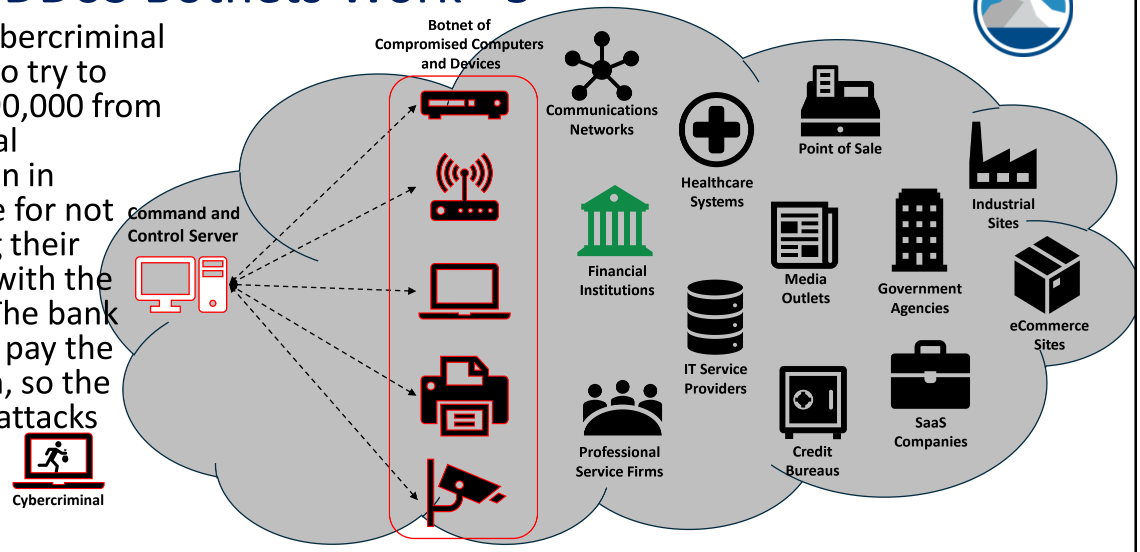
K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

How DDoS Botnets Work - 5

5. The cybercriminal decides to try to extort $90,000 from a financial institution in exchange for not attacking their website with the botnet. The bank does not pay the extortion, so the criminal attacks

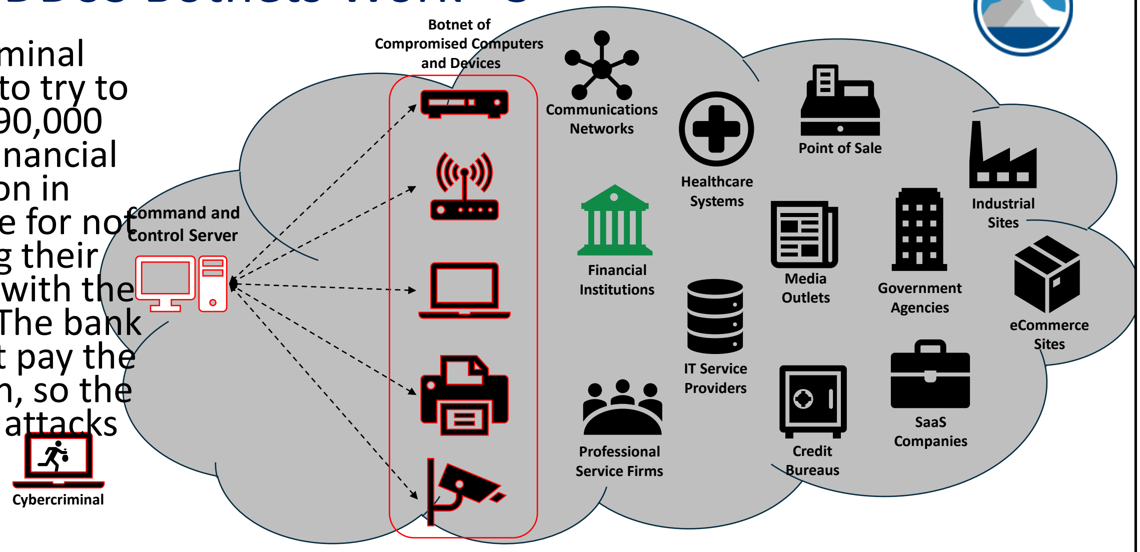


K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

How DDoS Botnets Work - 5

5. The cybercriminal decides to try to extort $90,000 from a financial institution in exchange for not attacking their website with the botnet. The bank does not pay the extortion, so the criminal attacks



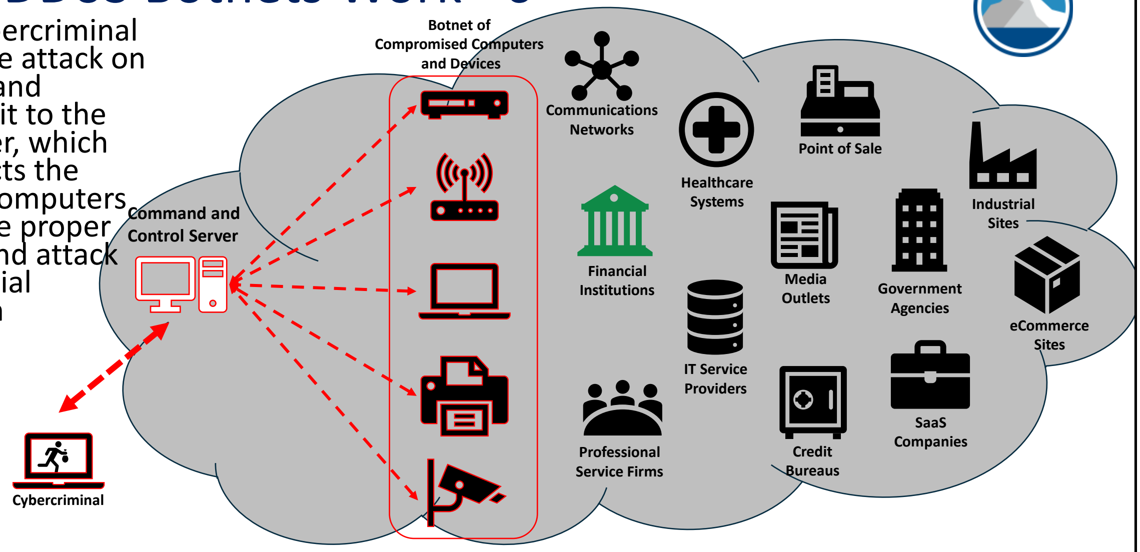
K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

How DDoS Botnets Work - 6

6. The cybercriminal sets up the attack on the bank and transmits it to the C&C server, which then directs the infected computers to load the proper exploits and attack the financial institution

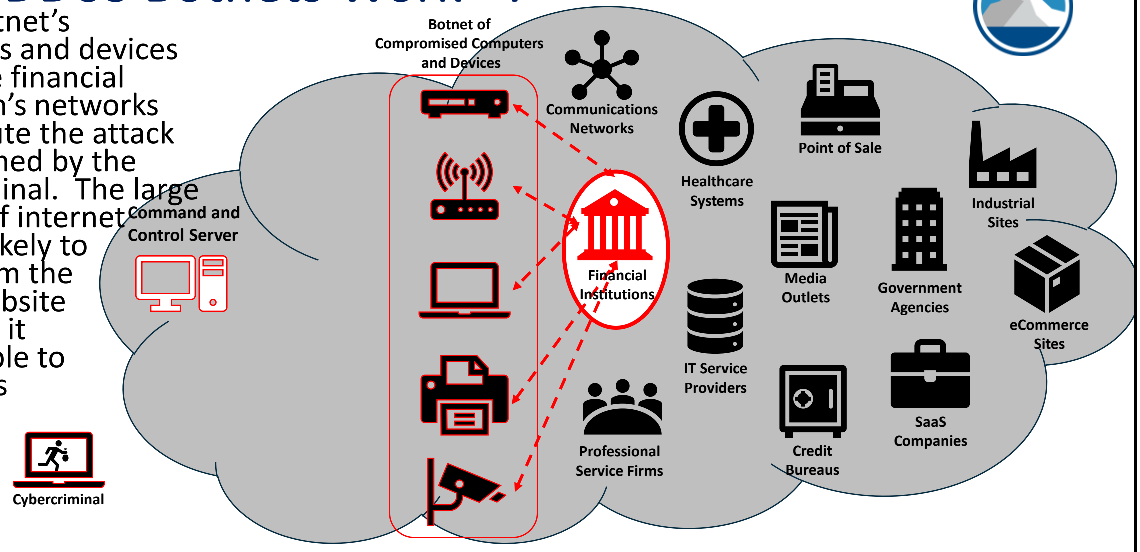


K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

How DDoS Botnets Work - 7

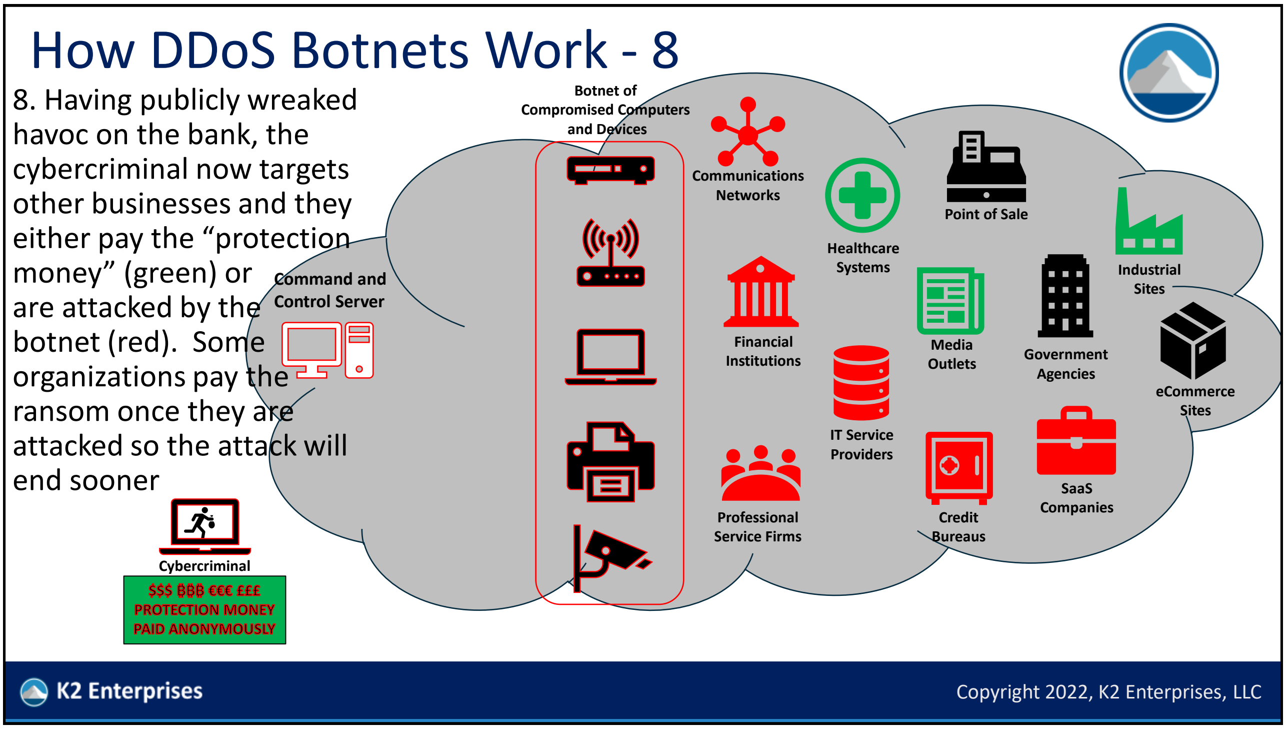
7. The botnet's computers and devices attack the financial institution's networks and execute the attack programmed by the cybercriminal. The large amount of internet traffic is likely to overwhelm the bank's website and make it inaccessible to customers



K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

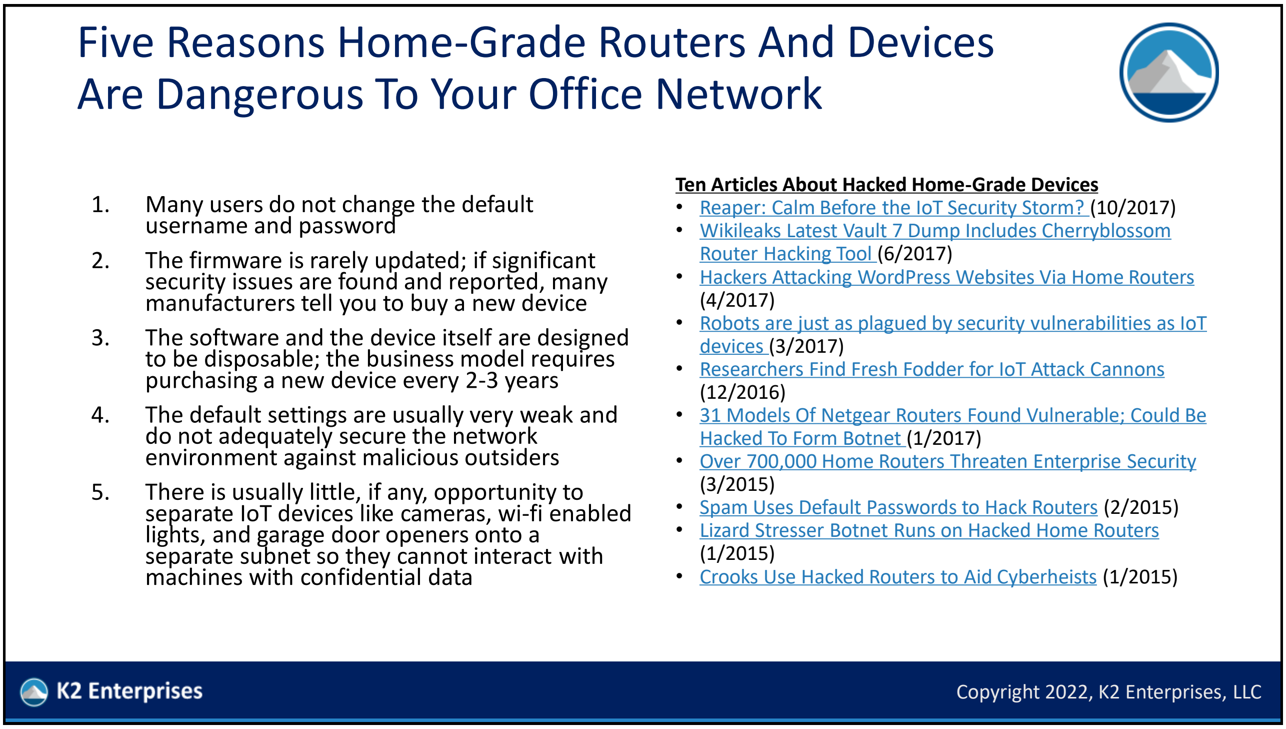
Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.



How DDoS Botnets Work - 8

8. Having publicly wreaked havoc on the bank, the cybercriminal now targets other businesses and they either pay the “protection money” (green) or are attacked by the botnet (red). Some organizations pay the ransom once they are attacked so the attack will end sooner

K2 Enterprises
Copyright 2022, K2 Enterprises, LLC



Five Reasons Home-Grade Routers And Devices Are Dangerous To Your Office Network

1. Many users do not change the default username and password
2. The firmware is rarely updated; if significant security issues are found and reported, many manufacturers tell you to buy a new device
3. The software and the device itself are designed to be disposable; the business model requires purchasing a new device every 2-3 years
4. The default settings are usually very weak and do not adequately secure the network environment against malicious outsiders
5. There is usually little, if any, opportunity to separate IoT devices like cameras, wi-fi enabled lights, and garage door openers onto a separate subnet so they cannot interact with machines with confidential data

Ten Articles About Hacked Home-Grade Devices

- Reaper: Calm Before the IoT Security Storm? (10/2017)
- Wikileaks Latest Vault 7 Dump Includes Cherryblossom Router Hacking Tool (6/2017)
- Hackers Attacking WordPress Websites Via Home Routers (4/2017)
- Robots are just as plagued by security vulnerabilities as IoT devices (3/2017)
- Researchers Find Fresh Fodder for IoT Attack Cannons (12/2016)
- 31 Models Of Netgear Routers Found Vulnerable; Could Be Hacked To Form Botnet (1/2017)
- Over 700,000 Home Routers Threaten Enterprise Security (3/2015)
- Spam Uses Default Passwords to Hack Routers (2/2015)
- Lizard Stresser Botnet Runs on Hacked Home Routers (1/2015)
- Crooks Use Hacked Routers to Aid Cyberheists (1/2015)

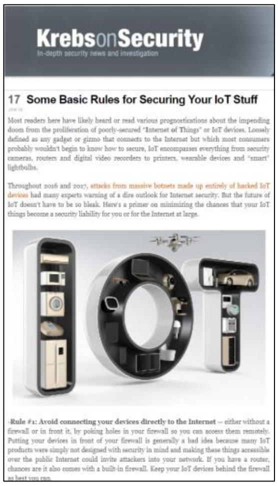
K2 Enterprises
Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Some Basic Rules For Securing Your IoT Stuff

(Adapted from Krebs on Security, 1/17/2018)

1. Avoid connecting your devices directly to the internet, and use a firewall to block incoming traffic
2. If you can, change the thing's default credentials
3. Update the firmware when you set up and also check for updates periodically
4. Check the default settings and make sure that features like UPnP are disabled
5. Avoid IoT devices that advertise Peer-to-Peer (P2P) capabilities to other devices or online
6. Consider the cost of the device – cheaper is usually not better



KrebsonSecurity
In-depth security news and investigation

17 Some Basic Rules for Securing Your IoT Stuff

Most readers here have likely heard or read various prognostications about the impending doom from the proliferation of poorly-secured "Internet of Things" or IoT devices. Loosely defined as any gadget or gizmo that connects to the Internet but which most consumers probably wouldn't begin to know how to secure, IoT encompasses everything from security cameras, routers and digital video recorders to printers, wearable devices and "smart" lightbulbs.

Throughout 2016 and 2017, attacks from massive botnets made up entirely of hacked IoT devices had many experts warning of a dire outlook for Internet security. But the future of IoT doesn't have to be so bleak. Here's a primer on minimizing the chances that your IoT things become a security liability for you or for the Internet at large.

Rule #1: Avoid connecting your devices directly to the Internet – either without a firewall or in front it, by poking holes in your firewall so you can access them remotely. Putting your devices in front of your firewall is generally a bad idea because many IoT products were simply not designed with security in mind and making these things accessible over the public Internet could invite attackers into your network. If you have a router, chances are it also comes with a built-in firewall. Keep your IoT devices behind the firewall as best you can.

Lessons Learned:

- Don't use home grade hardware anywhere in your business network unless its segmented onto a separate network which does not carry any confidential information
- Always change the default admin password on your router and other devices to a unique strong password which you store in password management software
- Keep the firmware in your devices updated to the latest versions to protect against known security issues on these devices
- Troubleshoot devices which are not performing properly and reconfigure/replace them promptly when trouble arises

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

"Gift Card Gang Extracts Cash from 100K Inboxes Daily",
Krebs on Security, September 2, 2021

KrebsonSecurity
In-depth security news and investigation

E-MAIL ACCOUNTS COMPROMISED, MINED FOR DATA

Copyright 2022, K2 Enterprises, LLC

What Happened?

- A cybercrime group targets e-mail account compromises and mines the accounts for valuable information in messages
  - The group purchases databases of usernames and passwords online which they use in credential stuffing attacks
  - They try between five and ten million of the usernames and passwords against webmail sites
  - The report claims that they compromise 50,000 to 100,000 new e-mail accounts ***every day***
  - Once e-mail accounts are compromised, they run searches against the stored messages (IMAP) to try to find valuable data

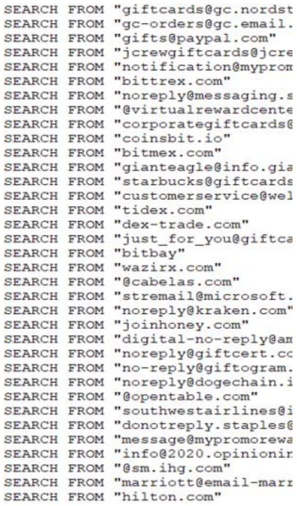
Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

What Do The Hackers Do With Accounts?

The group scans the messages in the account to look for things they can exploit:

- Gift cards delivered electronically that can be sold online
- E-mail messages from websites where they could steal personal data
- Items from cryptocurrency exchanges (e.g. Kraken or payment services (PayPal, Venmo, or bank-related services like Zelle)
- Frequent customer information which could help the hackers steal the points and sell them online

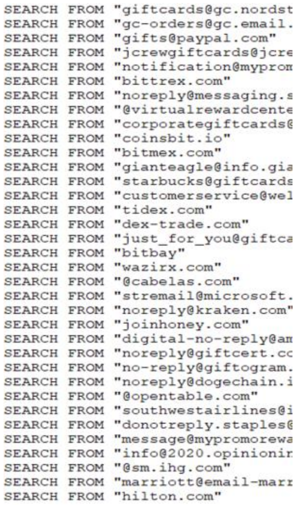


```
SEARCH FROM "giftcards@gc.nordst
SEARCH FROM "gc-orders@gc.email.
SEARCH FROM "gifts@paypal.com"
SEARCH FROM "jcrewgiftcards@jcre
SEARCH FROM "notification@myprom
SEARCH FROM "bittrex.com"
SEARCH FROM "noreply@messaging.s
SEARCH FROM "@virtualrewardcente
SEARCH FROM "corporategiftcards@
SEARCH FROM "coinsbit.io"
SEARCH FROM "bitmex.com"
SEARCH FROM "gianteagle@info.gia
SEARCH FROM "starbucks@giftcards
SEARCH FROM "customerservice@wel
SEARCH FROM "tidex.com"
SEARCH FROM "dex-trade.com"
SEARCH FROM "just_for_you@giftca
SEARCH FROM "bitbay"
SEARCH FROM "wazirx.com"
SEARCH FROM "@cabelas.com"
SEARCH FROM "stremail@microsoft.
SEARCH FROM "noreply@kraken.com"
SEARCH FROM "joinhoney.com"
SEARCH FROM "digital-no-reply@am
SEARCH FROM "noreply@giftcert.cc
SEARCH FROM "no-reply@giftogram.
SEARCH FROM "noreply@dogechain.i
SEARCH FROM "@opentable.com"
SEARCH FROM "southwestairlines@i
SEARCH FROM "donotreply.staples@
SEARCH FROM "message@mypromorewa
SEARCH FROM "info@2020.opinionin
SEARCH FROM "@sm.ihg.com"
SEARCH FROM "marriott@email-marr
SEARCH FROM "hilton.com"
```

What Accounts Are Targeted?

A list published as part of this story included 2,000 search terms which are applied against compromised accounts, including:

- Key retail brands targeted by searches include Cabelas, Nordstrom, Amazon, Apple, Best Buy, and virtually any retailer who offers gift cards to customers
- Financial institutions like Wells Fargo, Fidelity Investments, and many bank-related award sites
- Major cryptocurrency exchanges like Kraken, BitBay, Bitfinex, Crypto.com, and Dex-Trade
- Hospitality brands like most major airlines, hotel chains

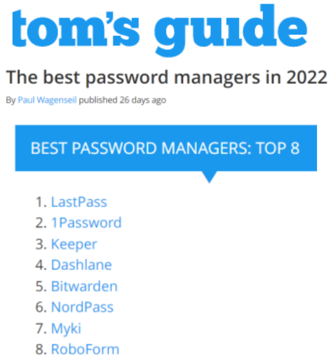


```
SEARCH FROM "giftcards@gc.nordst
SEARCH FROM "gc-orders@gc.email.
SEARCH FROM "gifts@paypal.com"
SEARCH FROM "jcrewgiftcards@jcre
SEARCH FROM "notification@myprom
SEARCH FROM "bittrex.com"
SEARCH FROM "noreply@messaging.s
SEARCH FROM "@virtualrewardcente
SEARCH FROM "corporategiftcards@
SEARCH FROM "coinsbit.io"
SEARCH FROM "bitmex.com"
SEARCH FROM "gianteagle@info.gia
SEARCH FROM "starbucks@giftcards
SEARCH FROM "customerservice@wel
SEARCH FROM "tidex.com"
SEARCH FROM "dex-trade.com"
SEARCH FROM "just_for_you@giftca
SEARCH FROM "bitbay"
SEARCH FROM "wazirx.com"
SEARCH FROM "@cabelas.com"
SEARCH FROM "stremail@microsoft.
SEARCH FROM "noreply@kraken.com"
SEARCH FROM "joinhoney.com"
SEARCH FROM "digital-no-reply@am
SEARCH FROM "noreply@giftcert.cc
SEARCH FROM "no-reply@giftogram.
SEARCH FROM "noreply@dogechain.i
SEARCH FROM "@opentable.com"
SEARCH FROM "southwestairlines@i
SEARCH FROM "donotreply.staples@
SEARCH FROM "message@mypromorewa
SEARCH FROM "info@2020.opinionin
SEARCH FROM "@sm.ihg.com"
SEARCH FROM "marriott@email-marr
SEARCH FROM "hilton.com"
```

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

How Should You Protect Yourself?

- Use password management software and have a different long/strong password for literally each account/website
- Wherever possible, activate “two factor authentication” (2FA) to protect your logins – in addition to username/password, have sites require additional proof before letting you log in – things like:
  - A code generated by a smartphone authenticator app
  - A hardware-based authentication USB key like a YubiKey or a Fido key
  - While having a code sent to your cell phone or a call to your phone is less secure than the above options, it is certainly better than no 2FA at all for the account



tom’s guide

The best password managers in 2022

By Paul Wagenseil published 26 days ago

BEST PASSWORD MANAGERS: TOP 8

1. LastPass
2. 1Password
3. Keeper
4. Dashlane
5. Bitwarden
6. NordPass
7. Myki
8. RoboForm

Credible review websites like PCMag.com or TomsGuide.com review and rank password managers so you can pick one and get to work immediately

K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

How Should You Protect Yourself?

- Avoid sending gift cards to e-mail – it’s not just impersonal, it makes your recipients subject to this kind of attack
  - When you do receive messages like this, retrieve the data on the gift card and either spend it quickly or print the code and delete the message
  - Do NOT leave the unredeemed code in your e-mail messages!
  - Don’t forget to empty your deleted items folder after deleting the message from your inbox

K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

“Ransomware Payments, Demands Rose Dramatically in 2021”,
Dark Reading, March 24, 2022

DARK Reading

RANSOMWARE PAYMENTS UP SIGNIFICANTLY IN 2021

K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

What Happened?

Palo Alto Networks’ Unit 42, a incident response vendor, reported on changes by ransomware attackers in 2021 as observed by their investigations team and as discovered on leak websites

- Ransomware attackers demanded higher ransom payments in 2021– up 144% to $2.2 million
- The average ransom payment made to attackers rose 78% to $541,010

UNIT 42

RANSOMWARE THREAT REPORT 2022

K2 Enterprises

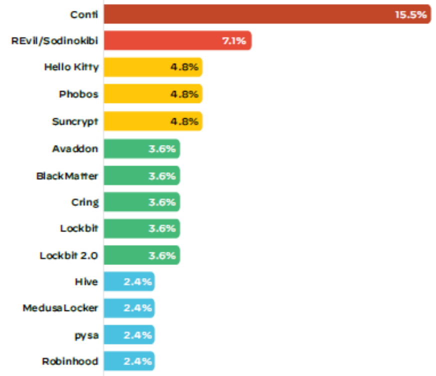
Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

What Happened?

- 85% of ransomware victims (2,566 companies) had their data dumped and exposed on leak websites – a “second chance” to get a ransom from victims
- 60% of victims were in the Americas, while 31% of targets were in Europe, Middle East, and Africa, and only 9% of those targeted were in the Asia/Pacific region
- Unit 42 found 35 new ransomware gangs in 2021 and the new gangs planned up to three different extortion attempts against victims – asking for ransoms to get decryption keys, not release data publicly, and finally a fee to avoid a distributed denial of service attack (DDoS) against the companies during their ransomware weakened state

Most Active Ransomware Variants in 2021



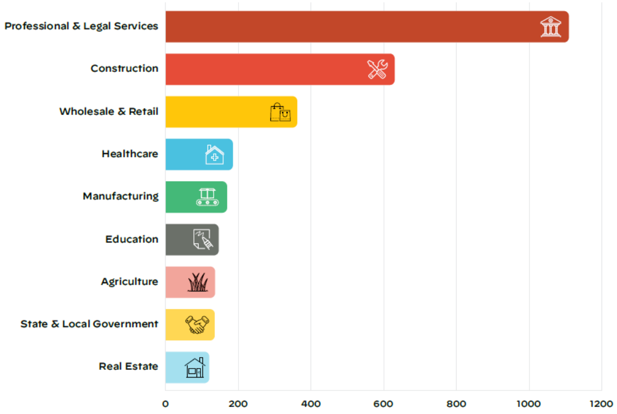
*(**Source**: Palo Alto Networks/Unit 42)*

K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

What Happened?

Sectors and Industries Most Heavily Targeted by Ransomware (from leak sites)



The most common industries targeted were:

- Professional services
- Construction,
- Wholesale/retail
- Healthcare
- Manufacturing

followed by Education, Agriculture, Government, and Real Estate

K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

How Should We Respond?

- There are no short cuts, and cybercriminal gangs will continue to innovate as they improve their operations – but the price of freedom is eternal vigilance
- Some of the basics which can mitigate some of the selected risks associated with ransomware include:
  - Have all employees and contractors take end user security awareness training and test the effectiveness of this training with e-mail tests
  - Require all administrators/superusers to use 2FA at all times
  - Don’t run unnecessary servers, and limit data/services exposed to the web
  - Keep your applications, operating systems, and the tools used to create custom applications up to date with the latest security updates
  - Evaluate your backup procedures and test the backup recovery procedures to gain assurance that your backups actually work
  - Have your network tested by credible penetration testers

K2 Enterprises
Copyright 2022, K2 Enterprises, LLC

IT WORLD CANADA

IT World Canada, November 21, 2019 (cpate.ch/brewbec)

ONTARIO BREWERY LOST $2.1 MILLION IN EMAIL BANK SCAM

K2 Enterprises
Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

What Happened?

- Waterloo Brewing in Waterloo, Ontario Canada fell victim to a “social engineering cyberattack” by a sophisticated third-party that resulted in the wire transfer of $2.1 million CAD in November 2019
- A perpetrator allegedly posed as an employee of a creditor for the brewery and requested the funds transfer to a different account, usually controlled by the perp
- The brewery tried and failed to recover the money, and has notified Waterloo Regional Police, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and the US Financial Crimes Enforcement Network (FINCEN)

K2 Enterprises Copyright 2022, K2 Enterprises, LLC

How Do Business E-mail Compromises Occur?

- Senior executives fall victim to spear phishing or whaling attacks allowing others to read their e-mail and determine how to use the hacked account to perpetrate a fraud
- For companies paying with wire transfers/ACH payments, someone calls the accounts payable department with an updated set of wire instructions to be used for payments
- Those responsible for banking transactions do not require procedures like two factor validation of authorization by a person known to them, authorization by two separate employees, or other internal controls

K2 Enterprises Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Tips On Avoiding Business E-mail Compromise

- Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail. For example, legitimate e-mail of *abc_company.com* would flag fraudulent e-mail of *abc-company.com*
- Create an e-mail rule to flag e-mail communications where the “reply” e-mail address is different from the “from” e-mail address shown
- Color code virtual correspondence so e-mails from employee/internal accounts are one color and e-mails from non-employee/external accounts are another
- Verify changes in vendor payment location by adding additional two-factor authentication such as having secondary sign-off by company personnel
- Confirm requests for transfers of funds by using phone verification as part of a two-factor authentication; use previously known numbers, not the numbers provided in the e-mail request
- Carefully scrutinize all e-mail requests for transfer of funds to determine if the requests are out of the ordinary

Source: FBI (cpate.ch/fbibec)

“A Hacker Got All My Texts for $16”, **Vice, March 15, 2021**

“Can We Stop Pretending SMS is Secure Now?”
Krebs on Security, November 19, 2021

SMS INTERCEPTION AND COMPROMISES USING BUSINESS TEXTING TOOLS

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

What Happened?

- A Vice reporter requested that a hacker take over his phone number to prove SMS message security vulnerabilities
- The hacker was able to redirect the messages from the reporter's cell phone and was also able to compromise many of that reporter's other accounts, including
  - The Bumble dating service
  - Meta's WhatsApp instant messaging service
  - Postmates food and grocery delivery service
- All of this was handled without any telltale activity to tip off the reporter that the compromise had occurred – the reporter's phone was on and connected to the carrier's network during the events – but no messages were received by the reporter

Copyright 2022, K2 Enterprises, LLC

How Did It Occur?

- The hacker used a prepaid credit card to pay $16/month to Sakari, one of many services which use the telephone network to allow businesses to send and receive marketing and sales text messages from a PC
  - Others in this segment include Beetexting & TextMyMainNumber
- The hacker forged the Letter of Authorization (LOA) for the reporter by filling in fake information purporting to be the reporter authorizing the redirection of the cell number to Sakari
- Sakari never validated that the number on the LOA matched the information with the carrier, nor did they text the reporter's cell phone number in this case (March 2021)

Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

What Should I Do?

- Don’t ever assume that your text messages are secure or that they are being delivered
- Don’t utilize SMS two factor authentication (2FA) tools and “log in with your phone number” solutions
- Consider not using a call or an SMS to your cell phone as a method for resetting your password on websites
- DO use other robust two-factor authentication methods like authentication apps, hardware devices like FIDO/YubiKey, and biometric authentication in addition to usernames and strong passwords to secure your accounts
- If you’re using business texting, you might consider a tool like Okey Monitor to monitor your phone numbers for unauthorized changes

“The ‘Zelle Fraud’ Scam: How it Works, How to Fight Back”
Krebs on Security, November 19, 2021

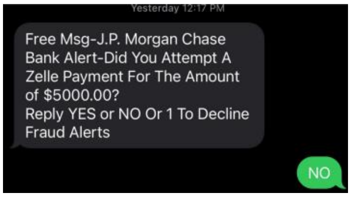
KrebsonSecurity
In-depth security news and investigation

VOICE SCAM FRAUD

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

What Happened?

- Cybercriminals are reportedly exploiting online peer to peer payment platforms like Zelle to drain victim bank accounts
- The criminals allegedly send SMS messages or call the victims, pretending to be an institution's fraud prevention department calling about a fake fraudulent transaction
- The criminals initiate the password reset process and initiate two-factor authentication regimes by creating fake SMS messages and calls to victims which gather SMS validation information and password reset data from the victim while the perpetrators are online resetting passwords, initiating transactions or otherwise advancing their scams
- The perpetrators reset the passwords, initiate the transfers, and are long gone before the fraud is discovered by the victim



Yesterday 12:17 PM

Free Msg-J.P. Morgan Chase Bank Alert-Did You Attempt A Zelle Payment For The Amount of $5000.00?
Reply YES or NO Or 1 To Decline Fraud Alerts

NO

Copyright 2022, K2 Enterprises, LLC

What Are The Implications?

- While businesses do not receive consumer fraud protections under Regulation E, CFPB has confirmed that banks and non-bank financial institutions are required to refund losses occurred in electronic funds transfers
- Banks are NOT required to refund losses related to transactions which they themselves initiated when fooled by fraudsters – these are NOT unauthorized transfers, since the transactions were confirmed by two factor authentication by the victims
- Frauds perpetrated on non-bank financial systems may make it harder for consumers to have institutions refund their losses from EFTs created under false pretenses

Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

"Intuit to Share Payroll Data from 1.4M Small Businesses With Equifax" **Krebs on Security, July 1, 2021**

"Fintech Startup Offers $500 for Payroll Passwords", **Krebs on Security, May 10, 2021**

KrebsonSecurity
In-depth security news and investigation

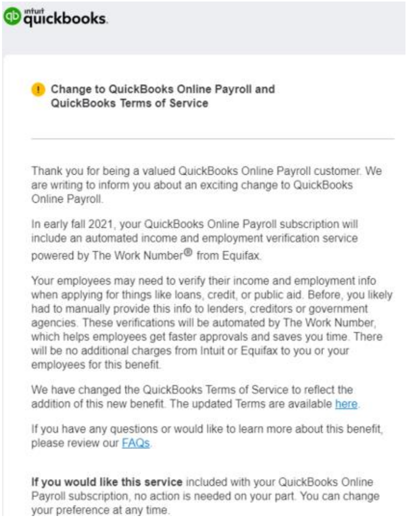
MISCELLANEOUS PRIVACY AND PRODUCTIVITY PERILS

K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

What Is Happening?

- Some technology companies are beginning to "by default" offer to share your employees' income and their employment status with credit bureaus as a "benefit" to the employer and employee (which provides the most benefit to the tech company, who can sell the formerly private data)



Change to QuickBooks Online Payroll and QuickBooks Terms of Service

Thank you for being a valued QuickBooks Online Payroll customer. We are writing to inform you about an exciting change to QuickBooks Online Payroll.

In early fall 2021, your QuickBooks Online Payroll subscription will include an automated income and employment verification service powered by The Work Number® from Equifax.

Your employees may need to verify their income and employment info when applying for things like loans, credit, or public aid. Before, you likely had to manually provide this info to lenders, creditors or government agencies. These verifications will be automated by The Work Number, which helps employees get faster approvals and saves you time. There will be no additional charges from Intuit or Equifax to you or your employees for this benefit.

We have changed the QuickBooks Terms of Service to reflect the addition of this new benefit. The updated Terms are available here.

If you have any questions or would like to learn more about this benefit, please review our FAQs.

If you would like this service included with your QuickBooks Online Payroll subscription, no action is needed on your part. You can change your preference at any time.

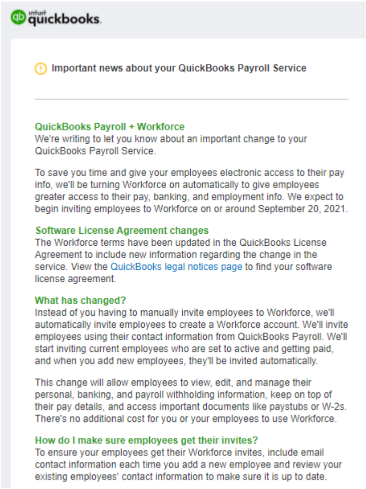
K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

What Is Happening?

- This privacy assault takes many forms:
  - Employees being offered by default payroll portals where the terms of service (TOS) and privacy policy indicate that the data can be combined with other data that the company has on the individual and will be shared with other Intuit subsidiaries like Credit Karma and Quicken Loans
  - Employers (and CPAs) are warned in junk mail-style messages that say that if you do nothing, your employees will be offered these portals – whose TOS/privacy policy the employees are unlikely to read and understand – so they are likely to consent without understanding the implications on the privacy of their data



Important news about your QuickBooks Payroll Service

QuickBooks Payroll + Workforce
We're writing to let you know about an important change to your QuickBooks Payroll Service.

To save you time and give your employees electronic access to their pay info, we'll be turning Workforce on automatically to give employees greater access to their pay, banking, and employment info. We expect to begin inviting employees to Workforce on or around September 20, 2021.

Software License Agreement changes
The Workforce terms have been updated in the QuickBooks License Agreement to include new information regarding the change in the service. View the QuickBooks legal notices page to find your software license agreement.

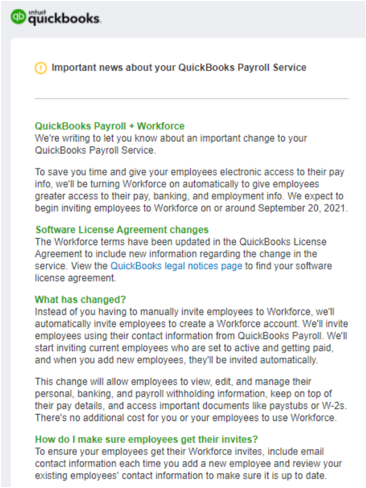
What has changed?
Instead of you having to manually invite employees to Workforce, we'll automatically invite employees to create a Workforce account. We'll invite employees using their contact information from QuickBooks Payroll. We'll start inviting current employees who are set to active and getting paid, and when you add new employees, they'll be invited automatically.

This change will allow employees to view, edit, and manage their personal, banking, and payroll withholding information, keep on top of their pay details, and access important documents like paystubs or W-2s. There's no additional cost for you or your employees to use Workforce.

How do I make sure employees get their invites?
To ensure your employees get their Workforce invites, include email contact information each time you add a new employee and review your existing employees' contact information to make sure it is up to date.

What Is Happening?

- This privacy assault takes many forms:
  - Employees being offered by default payroll portals where the terms of service (TOS) and privacy policy indicate that the data can be combined with other data that the company has on the individual and will be shared with other Intuit subsidiaries like Credit Karma and Quicken Loans
  - Employers (and CPAs) are warned in junk mail-style messages that say that if you do nothing, your employees will be offered these portals – whose TOS/privacy policy the employees are unlikely to read and understand – so they consent without understanding



Important news about your QuickBooks Payroll Service

QuickBooks Payroll + Workforce
We're writing to let you know about an important change to your QuickBooks Payroll Service.

To save you time and give your employees electronic access to their pay info, we'll be turning Workforce on automatically to give employees greater access to their pay, banking, and employment info. We expect to begin inviting employees to Workforce on or around September 20, 2021.

Software License Agreement changes
The Workforce terms have been updated in the QuickBooks License Agreement to include new information regarding the change in the service. View the QuickBooks legal notices page to find your software license agreement.

What has changed?
Instead of you having to manually invite employees to Workforce, we'll automatically invite employees to create a Workforce account. We'll invite employees using their contact information from QuickBooks Payroll. We'll start inviting current employees who are set to active and getting paid, and when you add new employees, they'll be invited automatically.

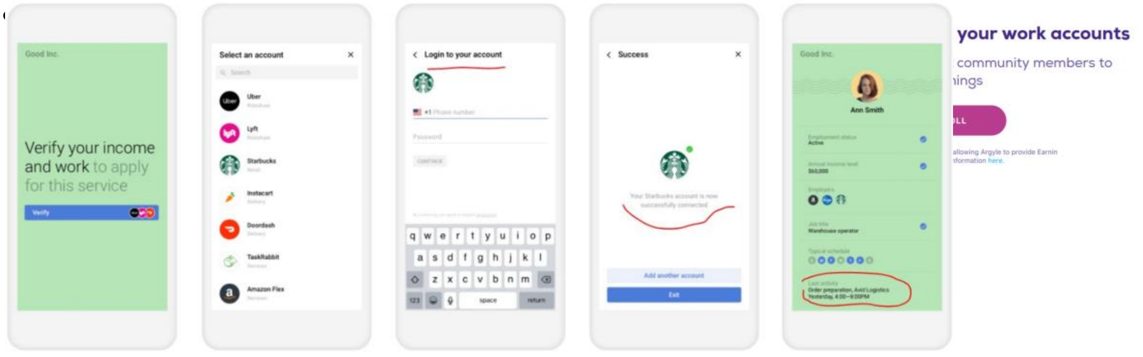
This change will allow employees to view, edit, and manage their personal, banking, and payroll withholding information, keep on top of their pay details, and access important documents like paystubs or W-2s. There's no additional cost for you or your employees to use Workforce.

How do I make sure employees get their invites?
To ensure your employees get their Workforce invites, include email contact information each time you add a new employee and review your existing employees' contact information to make sure it is up to date.

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

How it works

An example of Argyle Link integration into an app flow



Application

Argyle Link module

The user is asked to add their gig and employment accounts to verify income and work.

Argyle Link is surfaced to the user with a selection of gig and employment platforms.

A gig platform is successfully connected and work history data is being scanned in the

The user is presented with a custom product experience best on historic work data.

K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

How Should We Respond?

- It is critical that employees, employers, and their CPAs understand the privacy policies of the service providers which they use
- CPAs and business leaders should read and understand the terms of service, privacy policy, and should “opt out” of offering services to their employees which sell, store, and use their private payroll data to data brokers
- Some believe that accountants should avoid service providers whose business models include the sale of payroll data and other “validated data” to third parties or consumer lending affiliates

Steps to Opt Out of Data Verification in QB Online Payroll

1. Sign in to QuickBooks Online Payroll.
2. Go to Payroll Settings.
3. In the Shared data section, select the pencil and uncheck the box.
4. Select Save.

K2 Enterprises

Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

The End

QUESTIONS?

Copyright 2022, K2 Enterprises, LLC

Copyright © 2022. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.