COVID-19 and Cyber Heists: Financial System Under Attack

July 2020

Private and Confidential

vmware Carbon Black.

NORTON ROSE FULBRIGHT

Kroll | A Division of DUFF & PHELPS

DISCLAIMER

Any positions presented in this session are those of the panelists and do not represent the official position of Duff & Phelps, LLC or our co-hosts. This material is offered for educational purposes with the understanding that neither the authors nor Duff & Phelps, LLC or its affiliates are engaged in rendering legal, accounting or any other professional service through presentation of this material.

Speakers

KEITH WOJCIESZEK
Managing Director, Cyber Risk, Kroll

TOM KELLERMAN
Head of Cybersecurity Strategy, VMWare Carbon Black

WILL DAUGHERTY
Partner, data protection, privacy and cybersecurity group, Norton Rose Fulbright

Agenda

01

Threatscape

02

Destructive Attacks

03

Island Hopping

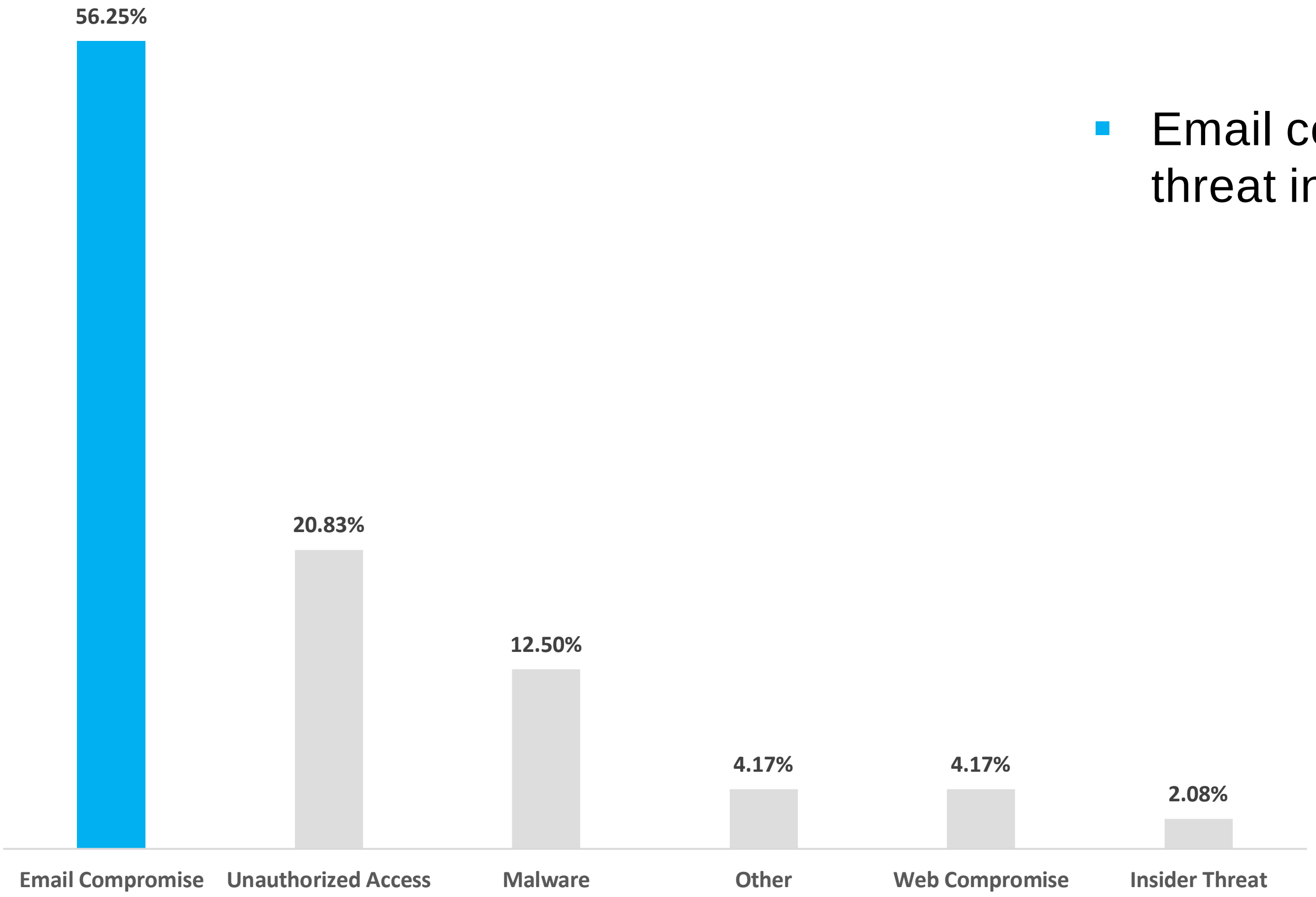
04

Access Mining

05

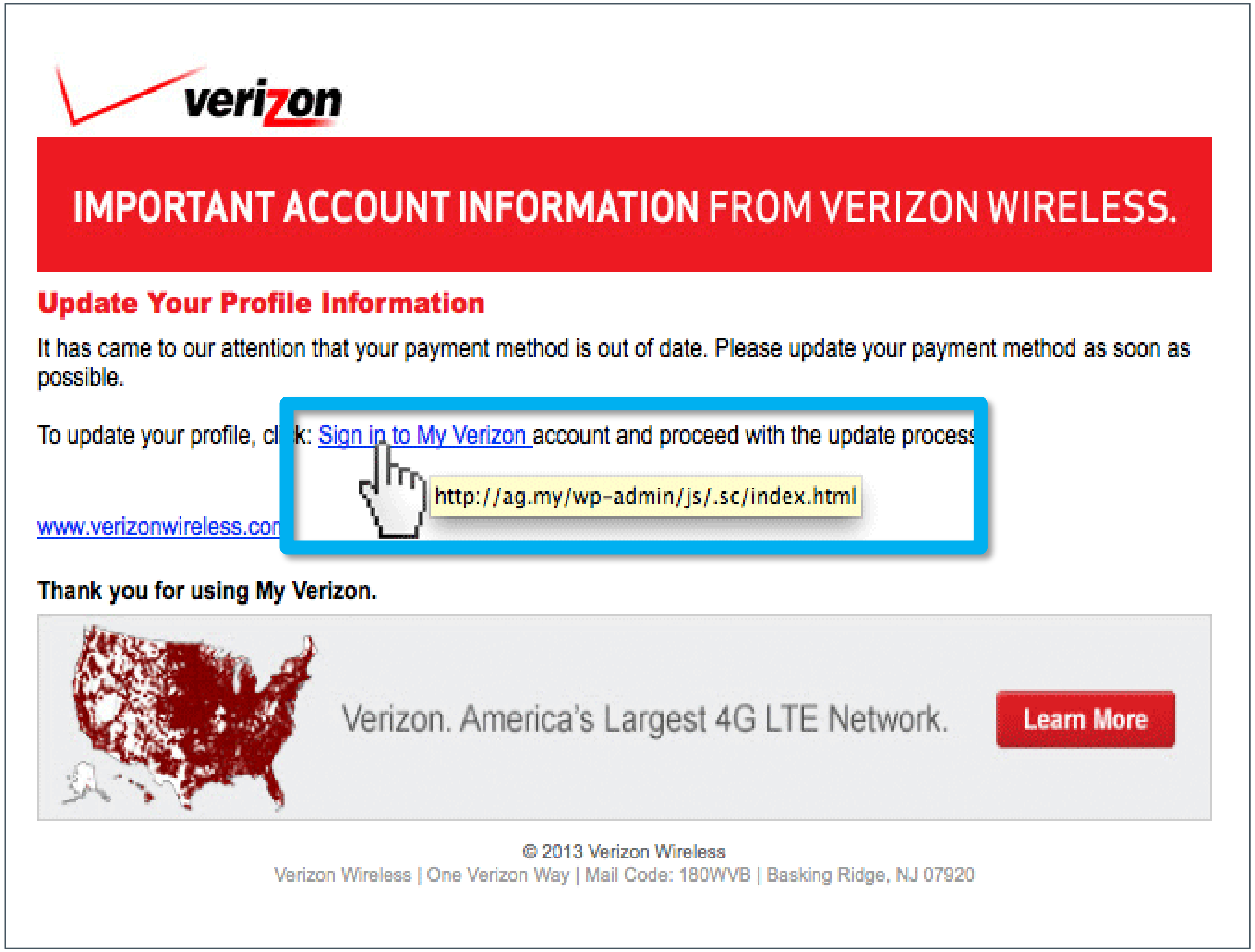
Investigations and Privilege

Financial Services by Threat Incident Type



- Email compromise was the most observed threat incident type YTD.

Realistic Templates



IMPORTANT ACCOUNT INFORMATION FROM VERIZON WIRELESS.

Update Your Profile Information

It has came to our attention that your payment method is out of date. Please update your payment method as soon as possible.

To update your profile, cl k: Sign in to My Verizon account and proceed with the update process

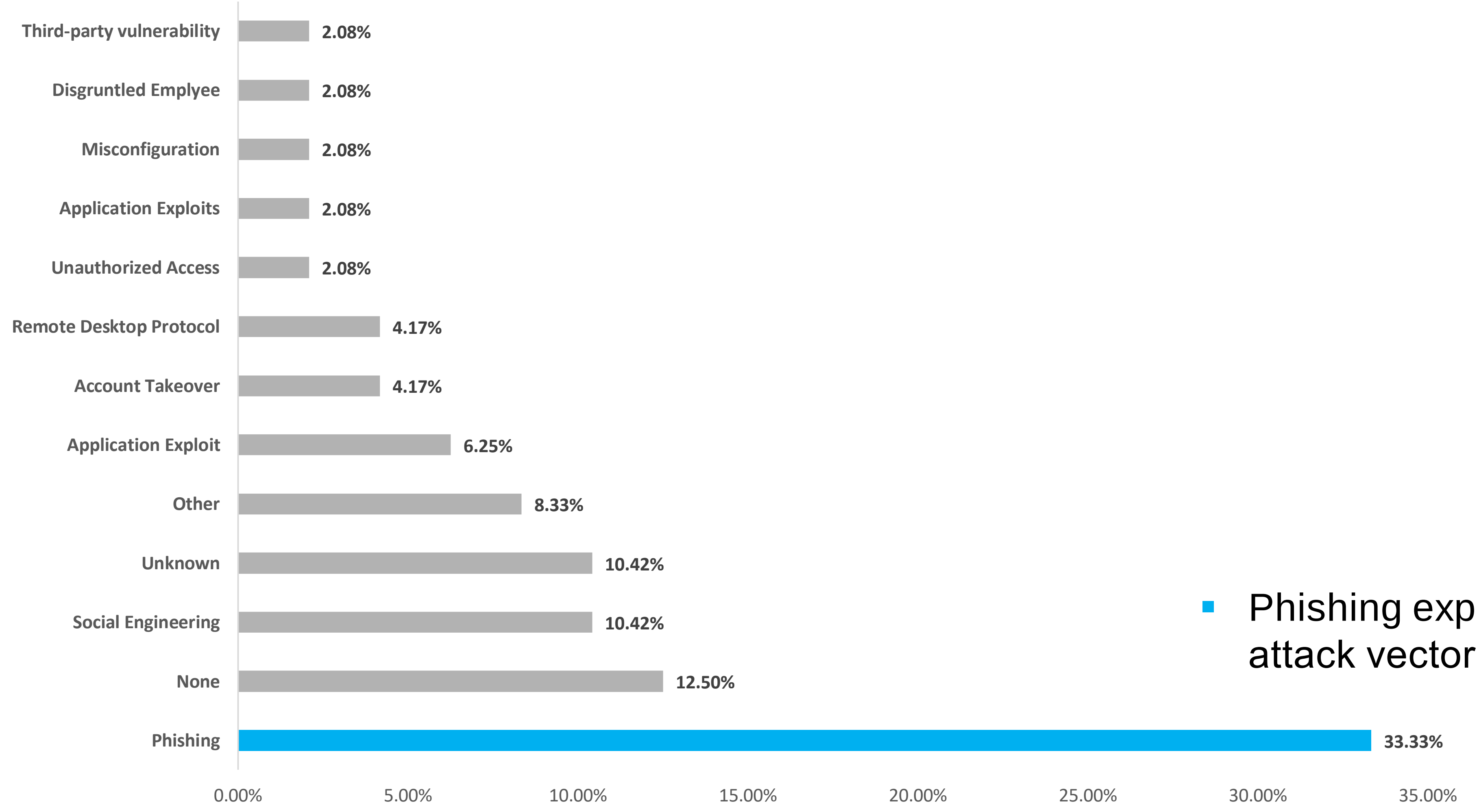
http://ag.my/wp-admin/js/.sc/index.html

www.verizonwireless.com

Thank you for using My Verizon.

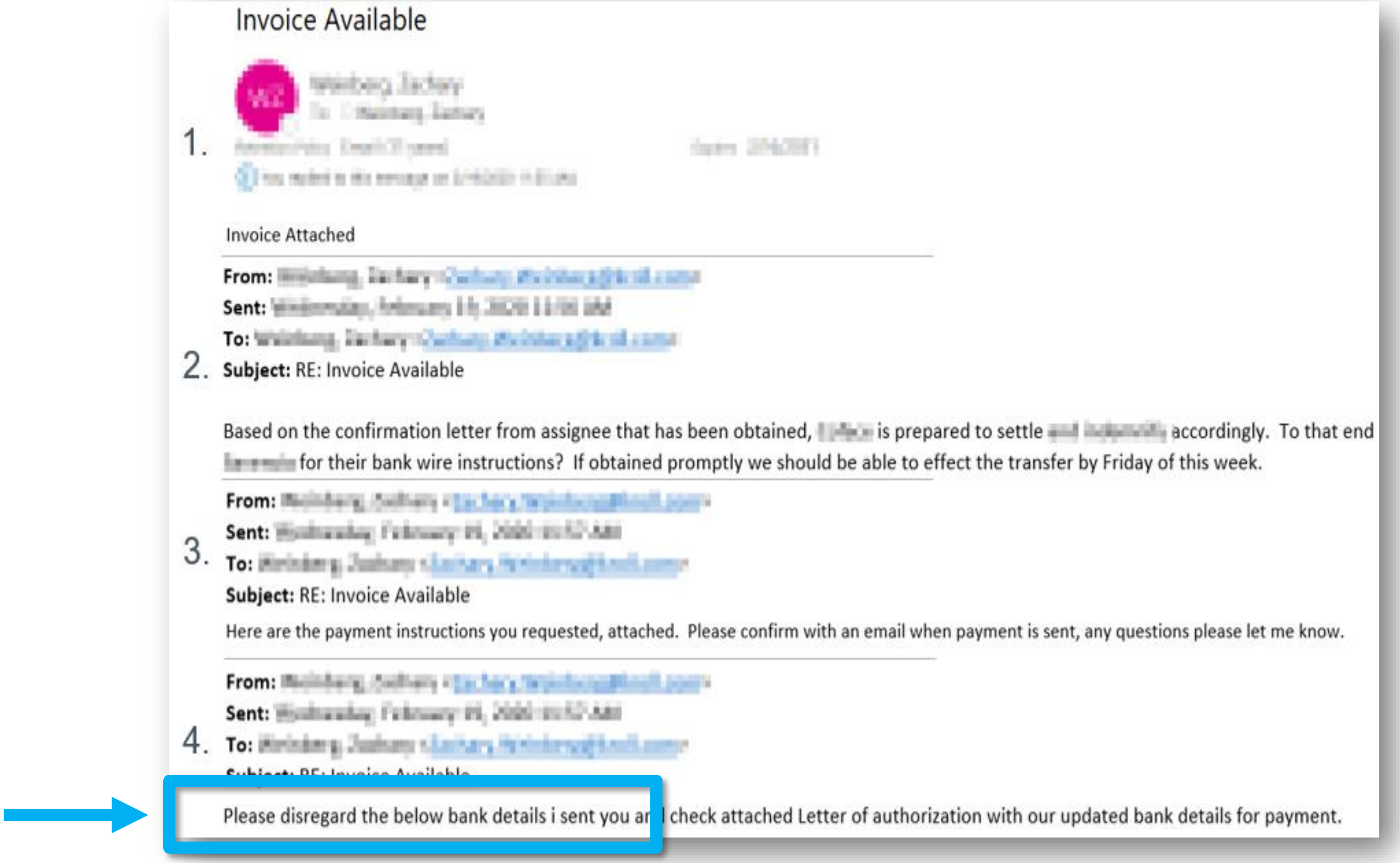
© 2013 Verizon Wireless
Verizon Wireless | One Verizon Way | Mail Code: 180WVB | Basking Ridge, NJ 07920

Financial Services by Infection Vector



- Phishing exploits were the leading attack vector in Kroll’s cases

Thread Hijacking Exponentially Increases Efficacy



Invoice Available

1. [redacted]

Invoice Attached

From: [redacted]
Sent: [redacted]
To: [redacted]
2. **Subject:** RE: Invoice Available

Based on the confirmation letter from assignee that has been obtained, [redacted] is prepared to settle [redacted] accordingly. To that end [redacted] for their bank wire instructions? If obtained promptly we should be able to effect the transfer by Friday of this week.

From: [redacted]
Sent: [redacted]
3. **To:** [redacted]
Subject: RE: Invoice Available

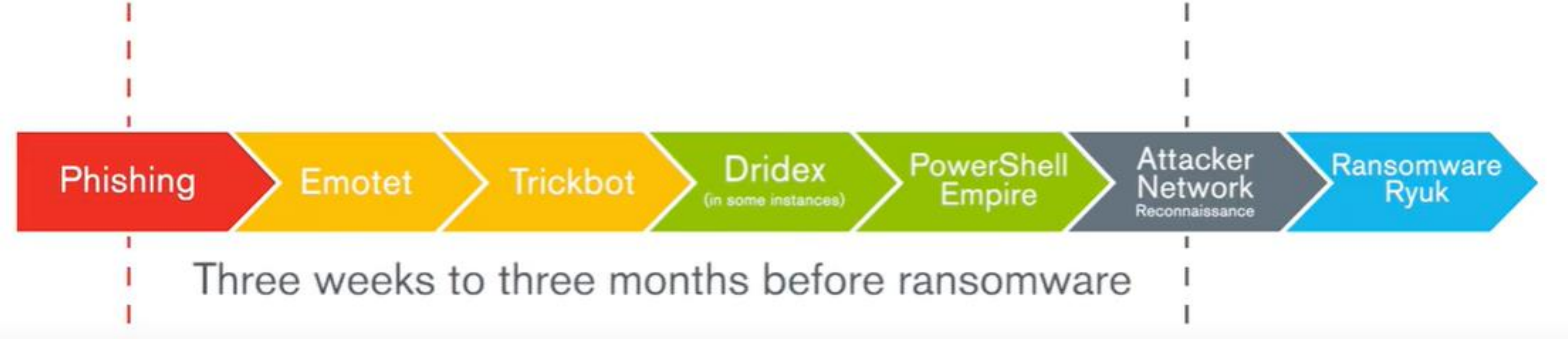
Here are the payment instructions you requested, attached. Please confirm with an email when payment is sent, any questions please let me know.

From: [redacted]
Sent: [redacted]
4. **To:** [redacted]
Subject: RE: Invoice Available

Please disregard the below bank details i sent you ar check attached Letter of authorization with our updated bank details for payment.

Destructive Attacks e.g. Attrition Has Increased 102%

Extracting as Much as Possible Before Detonating



- Sample observed timeline for Ryuk
- Similar patterns for Maze, Ragnar, etc.

Island Hopping Is Metastasizing

Your Digital Transformation will be Commandeered

3 Forms of “Island Hopping”

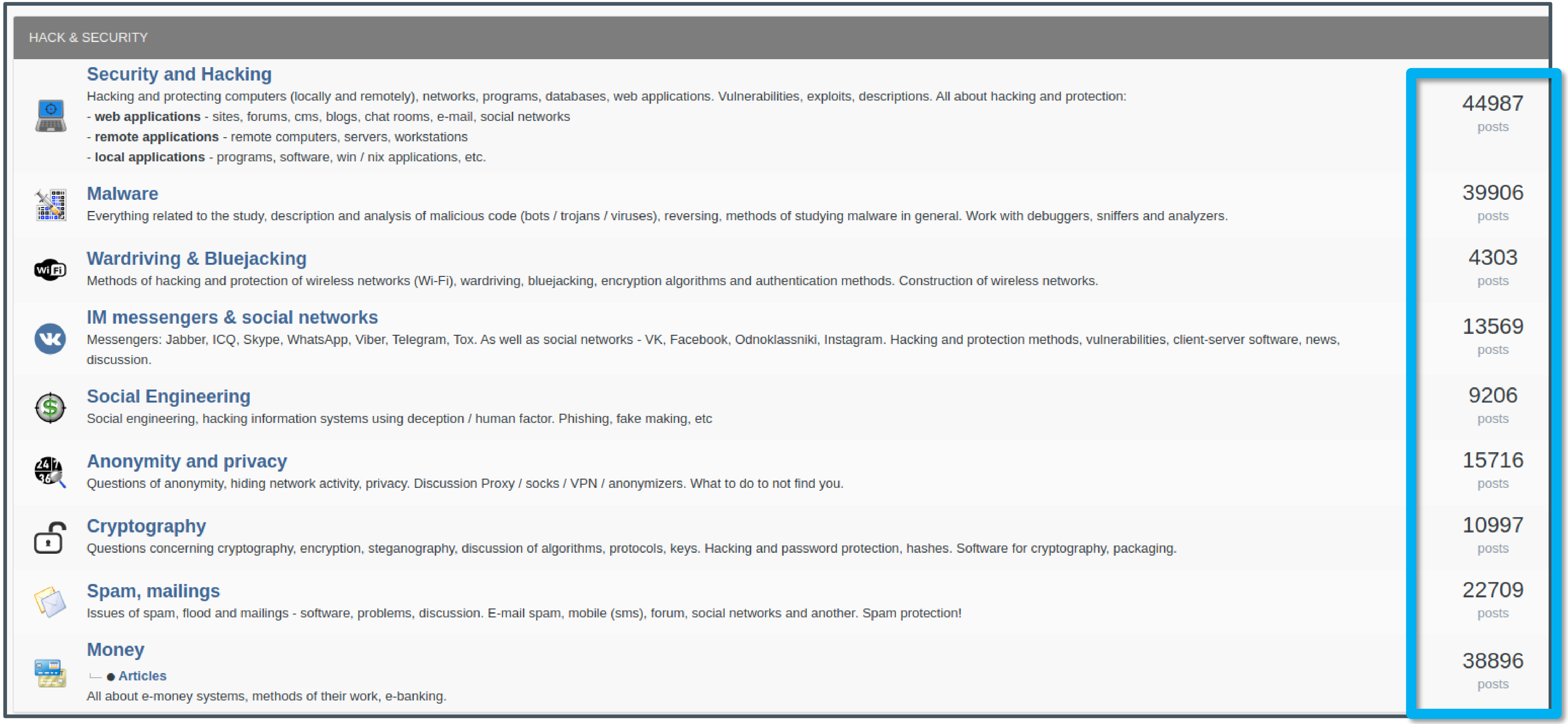
Network-based “island hopping”

Website converted into a “watering hole”

Reverse Business Email Compromise

Access Mining Marketplaces

It’s Never Been Easier to Buy Hacking Assistance and/or Tools



HACK & SECURITY

Security and Hacking

Hacking and protecting computers (locally and remotely), networks, programs, databases, web applications. Vulnerabilities, exploits, descriptions. All about hacking and protection:

- **web applications** - sites, forums, cms, blogs, chat rooms, e-mail, social networks
- **remote applications** - remote computers, servers, workstations
- **local applications** - programs, software, win / nix applications, etc.

44987 posts

Malware

Everything related to the study, description and analysis of malicious code (bots / trojans / viruses), reversing, methods of studying malware in general. Work with debuggers, sniffers and analyzers.

39906 posts

Wardriving & Bluejacking

Methods of hacking and protection of wireless networks (Wi-Fi), wardriving, bluejacking, encryption algorithms and authentication methods. Construction of wireless networks.

4303 posts

IM messengers & social networks

Messengers: Jabber, ICQ, Skype, WhatsApp, Viber, Telegram, Tox. As well as social networks - VK, Facebook, Odnoklassniki, Instagram. Hacking and protection methods, vulnerabilities, client-server software, news, discussion.

13569 posts

Social Engineering

Social engineering, hacking information systems using deception / human factor. Phishing, fake making, etc

9206 posts

Anonymity and privacy

Questions of anonymity, hiding network activity, privacy. Discussion Proxy / socks / VPN / anonymizers. What to do to not find you.

15716 posts

Cryptography

Questions concerning cryptography, encryption, steganography, discussion of algorithms, protocols, keys. Hacking and password protection, hashes. Software for cryptography, packaging.

10997 posts

Spam, mailings

Issues of spam, flood and mailings - software, problems, discussion. E-mail spam, mobile (sms), forum, social networks and another. Spam protection!

22709 posts

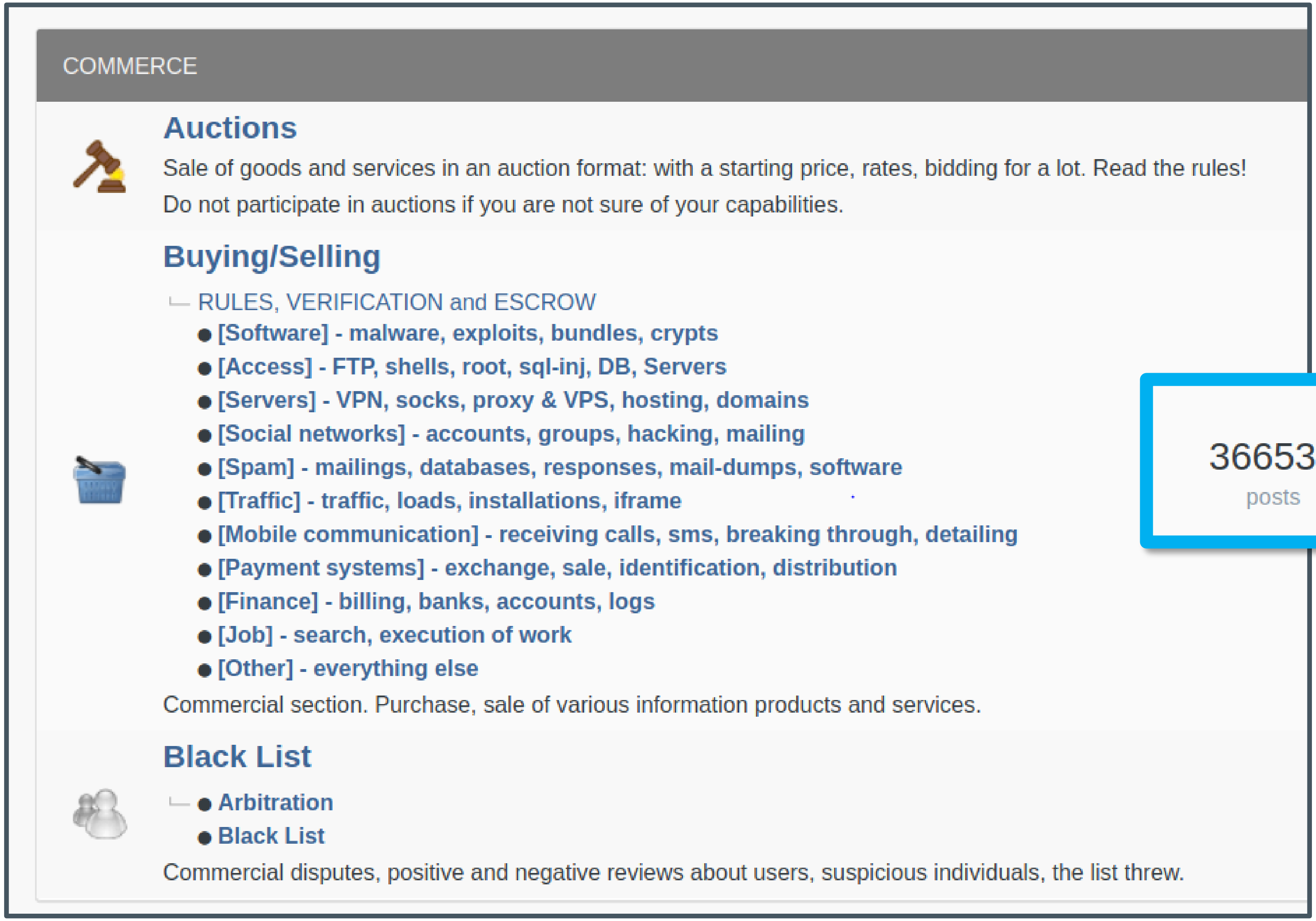
Money

└ ● **Articles**

All about e-money systems, methods of their work, e-banking.

38896 posts

Forums (Exploits, Malware, and data dump focused)



COMMERCE

Auctions

Sale of goods and services in an auction format: with a starting price, rates, bidding for a lot. Read the rules! Do not participate in auctions if you are not sure of your capabilities.

Buying/Selling

└ RULES, VERIFICATION and ESCROW

- ● [Software] - malware, exploits, bundles, crypts
- ● [Access] - FTP, shells, root, sql-inj, DB, Servers
- ● [Servers] - VPN, socks, proxy & VPS, hosting, domains
- ● [Social networks] - accounts, groups, hacking, mailing
- ● [Spam] - mailings, databases, responses, mail-dumps, software
- ● [Traffic] - traffic, loads, installations, iframe
- ● [Mobile communication] - receiving calls, sms, breaking through, detailing
- ● [Payment systems] - exchange, sale, identification, distribution
- ● [Finance] - billing, banks, accounts, logs
- ● [Job] - search, execution of work
- ● [Other] - everything else

Commercial section. Purchase, sale of various information products and services.

Black List

└ ● Arbitration

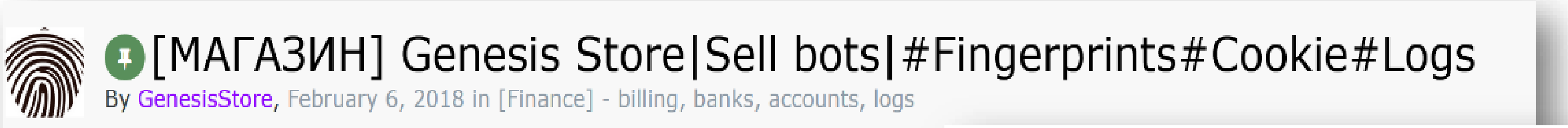
● Black List

Commercial disputes, positive and negative reviews about users, suspicious individuals, the list threw.

366535

posts

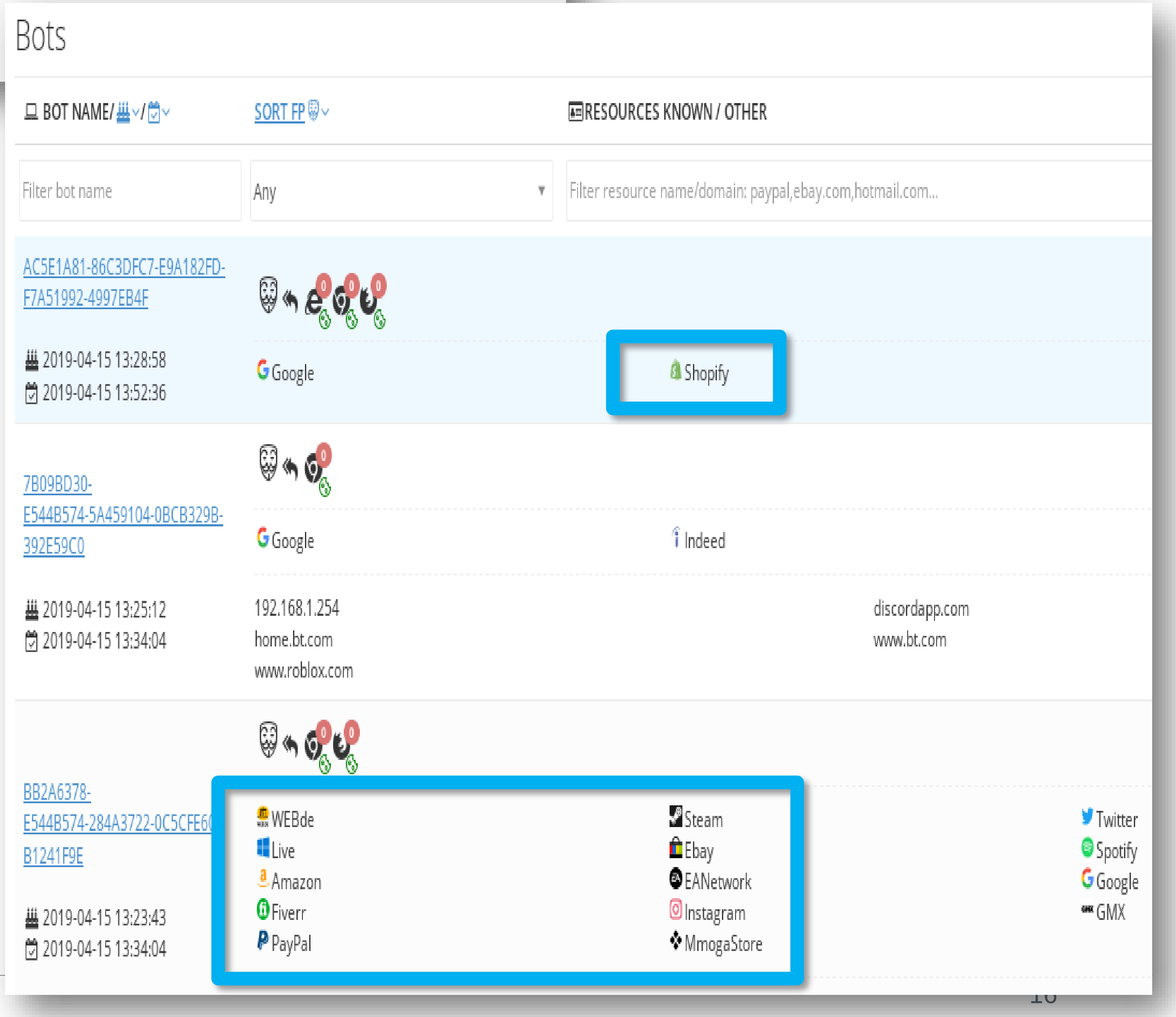
Monetization schemes exist for every type of stolen data



[МАГАЗИН] Genesis Store|Sell bots|#Fingerprints#Cookie#Logs

By GenesisStore, February 6, 2018 in [Finance] - billing, banks, accounts, logs

“Fingerprinted” browser IDs help bypass MFA



Bots

BOT NAME/ /	SORT FP	RESOURCES KNOWN / OTHER
Filter bot name	Any ▾	Filter resource name/domain: paypal,ebay.com,hotmail.com...
AC5E1A81-86C3DFC7-E9A182FD-F7A51992-4997EB4F 2019-04-15 13:28:58 2019-04-15 13:52:36	Google	Shopify
7B09BD30-E544B574-5A459104-0BCB329B-392E59C0 2019-04-15 13:25:12 2019-04-15 13:34:04	Google 192.168.1.254 home.bt.com www.roblox.com	Indeed discordapp.com www.bt.com
BB2A6378-E544B574-284A3722-0C5CFE6 B1241F9E 2019-04-15 13:23:43 2019-04-15 13:34:04	WEBde Live Amazon Fiverr PayPal	Steam Ebay EANetwork Instagram MmogaStore Twitter Spotify Google GMX

05

Investigations and Privilege

Moving Forward

SOPHISTICATED ATTACKS DEMAND SEASONED RESPONSE TEAM

- Custom malware, dark web marketplaces
- Access mining, island hopping, counter incident response

PRIVILEGE CONSIDERATIONS

- Current litigation decisions may impact privilege protection

SECURITY INTEGRATION

- Cyber and privacy converging throughout organization; security-first design

Q&A

KEITH WOJCIESZEK
Managing Director, Cyber Risk, Kroll

Keith.Wojcieszek@kroll.com

TOM KELLERMAN
Head of Cybersecurity Strategy, VMWare Carbon Black

tkellermann@vmware.com

WILL DAUGHERTY
Partner, data protection, privacy and cybersecurity group, Norton Rose Fulbright

Will.Daugherty@nortonrosefulbright.com

For more information about our global locations and services, please visit:

www.kroll.com

carbonblack.com

nortonrosefulbright.com

About Kroll

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security, and data and information management services. For more information, visit www.kroll.com.

About Duff & Phelps

Duff & Phelps is the global advisor that protects, restores and maximizes value for clients in the areas of valuation, corporate finance, investigations, disputes, cyber security, compliance and regulatory matters, and other governance-related issues. We work with clients across diverse sectors, mitigating risk to assets, operations and people. With Kroll, a division of Duff & Phelps since 2018, our firm has nearly 3,500 professionals in 28 countries around the world. For more information, visit www.duffandphelps.com.