Cyber Whaling – Part II

Why Should You (Really) Care About Cyber Whaling If You're A Business Executive, Board Member, Political Figure, Entrepreneur, or Government Official, aka "Organizational VIP?"

(For previous introductory and consecutive coverage of Cyber Whaling, see end of document)

Cyber Whaling Statistics:
Cyber whaling statistics are staggering and are getting worse. Consider these:

1. Cyber Whaling has become not just a highly lucrative profession for hackers but one that is highly effective at hurting you personally, as the "Whale" of your organization, and your organization itself. Oftentimes, you're not aware of this until it is too late.
2. Hackers use whaling to extract from you large money transfers or trade secrets (among others), monetizing any of which is highly lucrative. This is why FBI says "whaling attacks have seen a sharp rise and are expected to go up, [with resulting] losses of more than $12.5bn as of 2018," and that is significantly under-reported as not everyone has traditionally disclosed being a victim.
3. "Technical security solutions mostly fail to protect organizations against whaling attacks" because hackers use the power and authority of the Whale (the senior executive they're impersonating) to persuade people to do what is being asked without questioning details or looking too closely at the request and instead "just do as they're told."
4. 27% of respondents in a study said their CEOs had been the target, while 17% reported attacks on their CFO, both suggesting that most senior of the executive ranks are the favored targets of cybercriminals.
5. Whaling emails are more difficult to identify because many of these attacks don't include URLs or malicious attachments & generally rely exclusively on social-engineering to deceive their targets and bypass most of the security solutions**.** Therefore, many executives have fallen victim to specifically this attack vector.

Cyber Whalers (aka "Hackers") And Their Motivations:

The below diagram shows some of the main nation-state actors & their activities focused on whaling you.

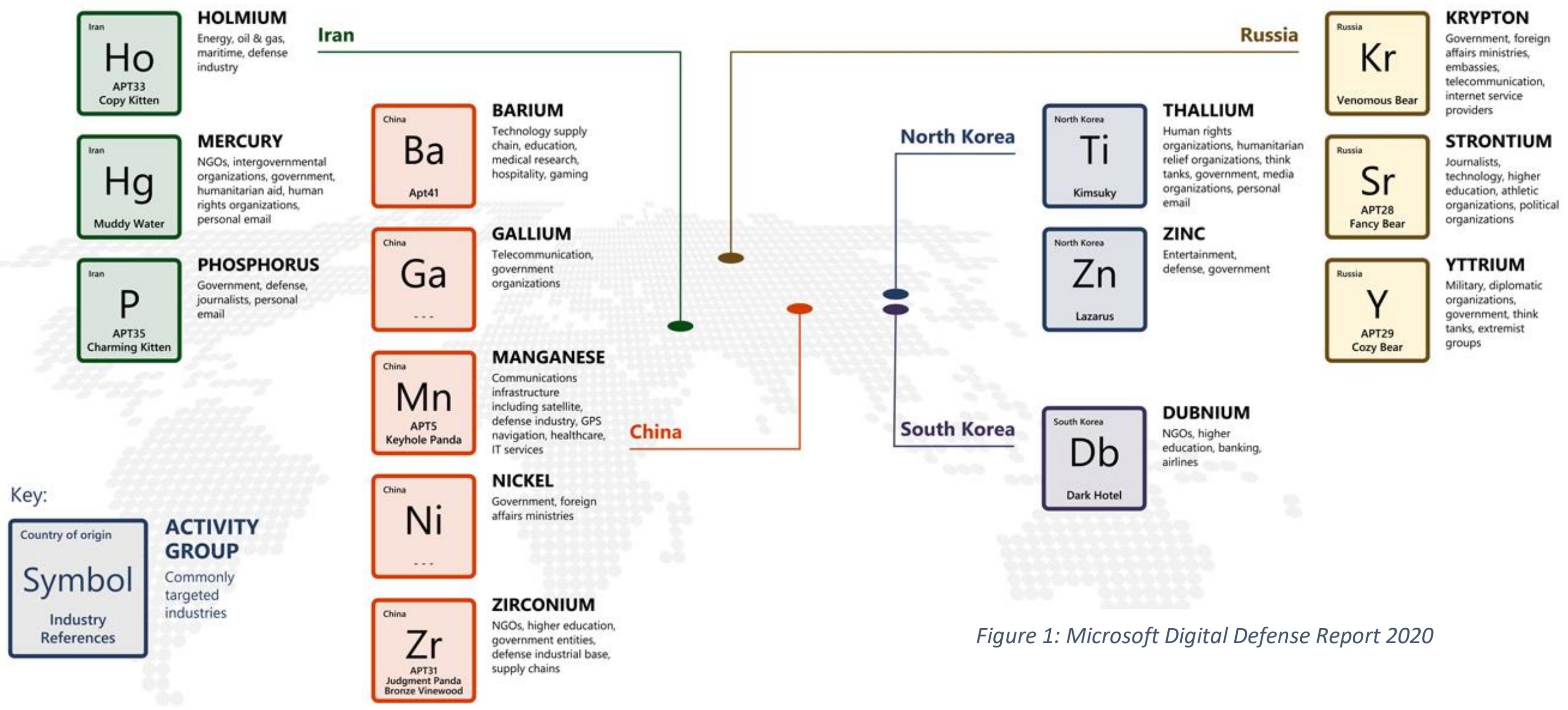
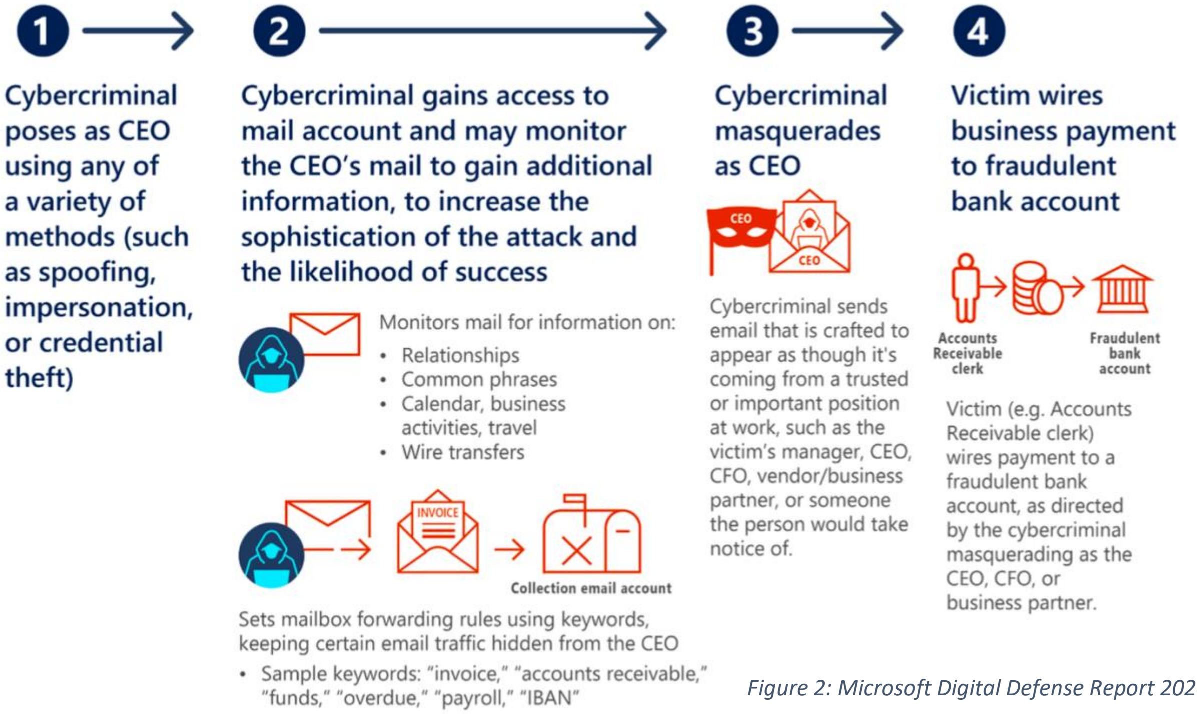

Iran
Ho
APT33
Copy Kitten
HOLMIUM
Energy, oil & gas, maritime, defense industry
Iran
Hg
Muddy Water
MERCURY
NGOs, intergovernmental organizations, government, humanitarian aid, human rights organizations, personal email
Iran
P
APT35
Charming Kitten
PHOSPHORUS
Government, defense, journalists, personal email
Iran
China
Ba
Apt41
BARIUM
Technology supply chain, education, medical research, hospitality, gaming
China
Ga
- - -
GALLIUM
Telecommunication, government organizations
China
Mn
APT5
Keyhole Panda
MANGANESE
Communications infrastructure including satellite, defense industry, GPS navigation, healthcare, IT services
China
China
Ni
- - -
NICKEL
Government, foreign affairs ministries
China
Zr
APT31
Judgment Panda
Bronze Vinewood
ZIRCONIUM
NGOs, higher education, government entities, defense industrial base, supply chains
Russia
North Korea
North Korea
Ti
Kimsuky
THALLIUM
Human rights organizations, humanitarian relief organizations, think tanks, government, media organizations, personal email
North Korea
Zn
Lazarus
ZINC
Entertainment, defense, government
South Korea
South Korea
Db
Dark Hotel
DUBNIUM
NGOs, higher education, banking, airlines
Russia
Kr
Venomous Bear
KRYPTON
Government, foreign affairs ministries, embassies, telecommunication, internet service providers
Russia
Sr
APT28
Fancy Bear
STRONTIUM
Journalists, technology, higher education, athletic organizations, political organizations
Russia
Y
APT29
Cozy Bear
YTTRIUM
Military, diplomatic organizations, government, think tanks, extremist groups
Key:
Country of origin
Symbol
Industry References
ACTIVITY GROUP
Commonly targeted industries

Figure 1: Microsoft Digital Defense Report 2020

A Typical Cyber Whaling Route:

Below diagram demonstrates a common, easily executable approach to attacking a whale & inducing compliance.



1 Cybercriminal poses as CEO using any of a variety of methods (such as spoofing, impersonation, or credential theft)

2 Cybercriminal gains access to mail account and may monitor the CEO's mail to gain additional information, to increase the sophistication of the attack and the likelihood of success

Monitors mail for information on:

- Relationships
- Common phrases
- Calendar, business activities, travel
- Wire transfers

Sets mailbox forwarding rules using keywords, keeping certain email traffic hidden from the CEO

- Sample keywords: "invoice," "accounts receivable," "funds," "overdue," "payroll," "IBAN"

3 Cybercriminal masquerades as CEO

Cybercriminal sends email that is crafted to appear as though it's coming from a trusted or important position at work, such as the victim's manager, CEO, CFO, vendor/business partner, or someone the person would take notice of.

4 Victim wires business payment to fraudulent bank account

Victim (e.g. Accounts Receivable clerk) wires payment to a fraudulent bank account, as directed by the cybercriminal masquerading as the CEO, CFO, or business partner.

Figure 2: Microsoft Digital Defense Report 2020

Your Risks in Being Cyber Whaled[1]:

1. **Financial Loss:** A principal objective is to extract money from targeted organizations. When second-order financial penalties (e.g. fines) are accounted for, whaling attacks can prove extremely damaging.
2. **Data Breach:** Data breaches are rarely out of the press these days. One of the scams that resonates most with the media is credential harvesting and the stealing of user data. With organizations now holding more information on individuals (employees and customers) than ever before, these attacks can cause immense harm to people and to businesses. What's more, data breaches are expensive to manage; the average cost of a breach is $3.9mm and as high as $350mm.
3. **Fines:** It's hard to think of data breaches and email attacks without the associated fines brought about by new regulation. In one of the first big GDPR fines, the UK's Information Commissioner earlier in 2019 announced its intention to fine British Airways £183 million after a 2018 data breach.
4. **Reputational Damage:** It's harder to quantify on a balance sheet, but after a whaling-induced data breach, hard-won brand reputation could be put at serious risk. An email security failure can negatively affect an organization's relationships with their customers. Another second-order effect could be knocking employees' morale and denting confidence, making rebuilding work still more difficult.

To access previous Cyber Whaling posts:

1) Part I – 2020.11.23: Why must business executives, Board Directors, politicians, entrepreneurs & other leaders focus on their cybersecurity differently than cybersecurity of their broader organization?
2) Intro – 2020.11.20: Why are Organizational VIPs such a perfect target for hackers and why am I therefore obsessed with helping leaders avoid these attacks?

About the Author: Mr. Cetnarski is a national & cyber security strategist, Founder & CEO of cyber defense ecosystem Cyber Nation Central® & Executive Producer of VIP Cybersecurity Blueprint™. Formerly an investment banker with UBS technology & real estate groups & Chairman/CEO of a global tech & hospitality venture, he is an alumnus of Harvard's Kennedy School of Government, The Wharton School, and the University of Chicago, and writes on integration of strategy, tech innovation, and policy in the areas of cybersecurity, national security, countering disinformation campaigns, and privacy.

[1] From https://www.tessian.com/blog/whaling-phishing-attack/