Killnet Attacks on U.S. Health Sector

Group 23: Michael Schwob, Brandon Weinerman, Jorja Szczerbinski, Nazman Rosman, Taylor Smith, Donald Wheeler

Introduction

Killnet

- Russian nationalist hacker group
- Attack government orgs and healthcare facilities of enemy countries
- Employ DDoS attacks to disrupt services and data exfiltration scripts to breach patient and employee privacy

Target

- U.S. Department of Health and Human Services, related Healthcare and Health Insurance orgs
- U.S. Health Sector is increasingly reliant on IT infrastructure to provide services
- Additional investment into IT infrastructure and cybersecurity needed to protect patient well-being and privacy

Timeline

2022

January 28th
Killnet attack list for hospitals and medical organizations are leaked, many of the hospitals/organization s being in U.S.

February 24th
Russia escalates war by invading Ukraine

February 25th
Killnet, in support of Russia declares war on hacktivist group Anonymous that supports Ukraine

December 8th
Killnet leader 'KillMilk' threatens to disable critical medical systems and to leak credit card information of millions of Americans

December 16th
Killnet attacks services of company Humana, a health insurance organization subsidized by the U.S. Department of Defense

2023

January 28th
Killnet threatens specific U.S. Healthcare companies and launches coordinated DDoS attacks against healthcare sectors of U.S and other NATO allies in response to military aid to Ukraine

UI Stead Family Children's Hospital and Carver College of Medicine were attacked and faced outages.

February 1st
Killnet invites affiliates to join their attack campaign, threatens U.S. and Europe with a 'huge surprise'

February 4th
Killnet leader (KillMilk) posts a meme, threatening the U.S. Department of Health and Human Services (HHS).

March 17th
Microsoft Security published its observations that Killnet had been targeting healthcare applications for the last three months using the Microsoft Azure infrastructure.

March 26th
Killnet leader (KillMilk) announces that "they had undergone a reform of personnel", hinting they were growing in size and support.

October 4th
ICRC issues 8 rules for cyber-warfare aimed to protect civilians. Several Russian and Ukrainian groups alike agree to these rules. Killnet vows to deescalate attacks against civilians.

Critical Infrastructure Overview

DDoS Attacks

- Done on healthcare services mainly in western areas
- Had a low cost and efficient way of hacking
- Anonymous attacks
- Kept growing

Protecting for the Future

- Enabling network protection
- Reaching out for help during an attack
- Knowing what to do in case something like this were to ever happen

Primary Asset, Protector & Threat

Assests

- Preservation of patient lives
  - Protect and care for patients as they recover from injury and illness
- Reputation
  - Trustworthy, responsible for vulnerable lives
  - Responsible for patient privacy

Protectors

- IT infrastructure of healthcare facilities
  - IT equipment and the security of their systems is essential to allowing healthcare facilities to operate smoothly
  - Weakened web servers and cyber security allow easy access for potential threats to harm the healthcare sector

Threats

- A series of DDoS attacks sent by Killnet's hacktivists
  - Floods the web servers of targeted healthcare facilities, making vital information unaccessible
  - Hinders healthcare professionals ability to provide life-saving care
- Blackmail
  - Goal is to pressure the target into paying to stop the attack

American Hospital Association, 2023

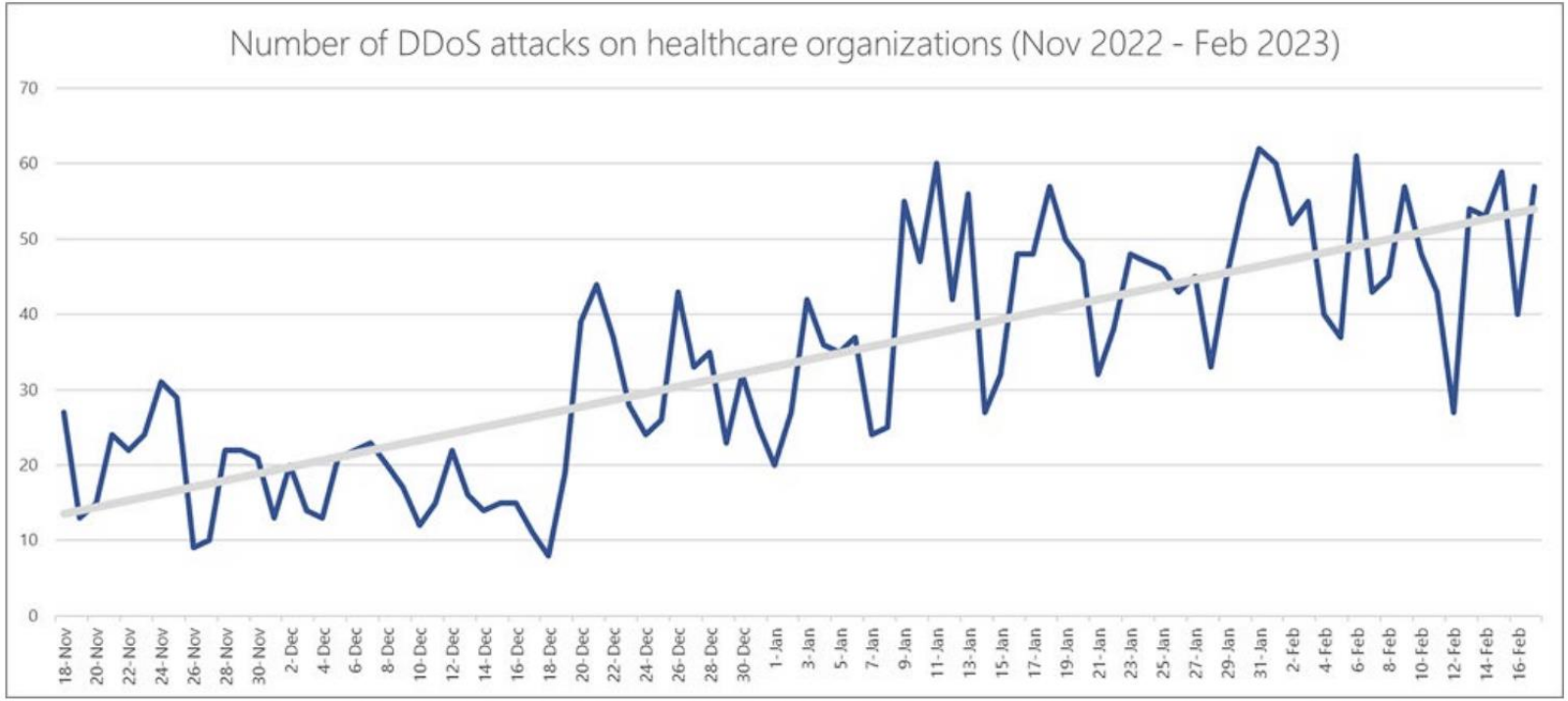


Figure 12: Microsoft Security graph of DDoS attacks on healthcare applications in Azure. (March 17, 2023)

- American Hospital Association. (2023, April 5). HC3 TLP clear analyst note: Pro-Russian hacktivist group threat to HPH sector January 30, 2023: AHA. https://www.aha.org/cybersecurity-government-intelligence-reports/2023-01-30-hc3-tlp-clear-analyst-note-pro-russian-hacktivist-group-threat-hph

Related Critical Infrastructures

Communications Sector

- Communcation between patients and providers became unavailable

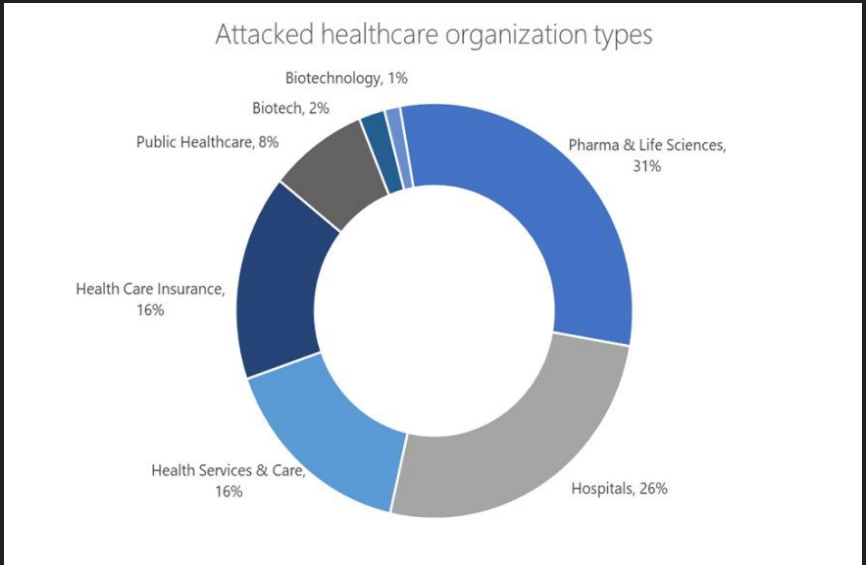
Information Technology Sector

- Crucial patient data became unavailable
- Disrupted medical processes like diagnosis, and planning treatments

Related Critical Infrastructures

Financial Sector

- Pharma and insurance firms lose revenue



Dahan, A., & Pasha, S. (2023, March 17). KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2023/03/17/killnet-and-affiliate-hacktivist-groups-targeting-healthcare-with-ddos-attacks/?msockid=27462cbff24a6244001c3859f338636d z

Related World Events

Russia-Ukraine War

- Killnet forms around same time Russia invades Ukraine
- They attack NATO members and allies of Ukraine
- U.S., providing aid to Ukraine becomes a natural target for them

COVID-19 Pandemic

- Healthcare sector extremely drained
- Resources diverted to handling virus leaving less for IT/Security
- Killnet able to capitalize on this increased vulnerability

ICRC Rules

- ICRC issues 8 rules for cyber-warfare
- Rules meant to protect civilians from becoming victims
- Both IT Army of Ukraine and Killnet vow to abide by rules

Intelligence Strategies

Red Cell Analysis

- You need to think like the hacker, to eliminate the risk of a breach.
- Think in the hackers perspective
- Who should we target?
- How should we target them?
- When should we target them?
- What information are we interested in?

SIGINT

Signals Intelligence

- Need to gather intelligence data, messages, or other digital footprints to further understand the hacker's footprints and their intentions/goals further
- Figure out how, when, and why they are going to attack, allows a warning for healthcare service

Risk Analysis and Recommendations

Prevention

Install Anycast network systems and limiting outside traffic use.

Pros:

Protects our information and data on the computer

Manually can overthrow the DDoS attack and limits risk for future threats

Limits money for repairs after that attacks that would take place on the devices

Cons:

Protection against all DDoS attacks are not guaranteed

Having to spend money to train employees on how to navigate the new tech

Out of date software leaves our systems vulnerable

Mitigation

Install OVHcloud to have servers and networks to block the DDoS "Flood".

Pros:

It is a non-manual function not having to keep someone monitoring it

Allows for the computer to still function while an attack is going on

Doesn't slow down the hospital's efficiency

Cons:

Doesn't protect against all DDoS attacks certain one may be able to break through

Once KillNet or other groups are aware of the method used to get through it will be hard to stop them

Our network and server will have to be replaced due to outdated systems at some point.

Summary

- Killnet's DDoS attacks affected tons

- Having secure and protected websites is crucial to preventing future attacks
- Ex. Adding firewalls for protection

- If more healthcare services had been attacked, more people would have been exposed and at risk.

References

- Al-Aboosi, A. M. M., Abdullah, S. N. H. S., Murah, M. Z., & Dharhani, G. S. A. (2022, October 6-7). Cybersecurity Trends in Health Information Systems. 2022 International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates. https://ieeexplore-ieee-org.ezaccess.libraries.psu.edu/document/9995952

- American Hospital Association. (2023, April 5). HC3 TLP clear analyst note: Pro-Russian hacktivist group threat to HPH sector January 30, 2023: AHA. https://www.aha.org/cybersecurity-government-intelligence-reports/2023-01-30-hc3-tlp-clear-analyst-note-pro-russian-hacktivist-group-threat-hph

- Cloudflare. (n.d.). How to prevent ddos attacks | methods and tools. Cloudflare. https://www.cloudflare.com/learning/ddos/how-to-prevent-ddos-attacks/

- Dahan, A., & Pasha, S. (2023, March 17). KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2023/03/17/killnet-and-affiliate-hacktivist-groups-targeting-healthcare-with-ddos-attacks/?msockid=27462cbff24a6244001c3859f338636d

- Flashpoint. (n.d.). Killnet: Inside the World's Most Prominent Pro-Kremlin Hacktivist Collective. Flashpoint. https://flashpoint.io/intelligence-101/killnet/

References (cont.)

- Forescout. (n.d.). Killnet: Analysis of Attacks from a Prominent Pro-Russian Hacktivist Group. Forescout Vedere Labs. https://www.forescout.com/resources/analysis-of-killnet-report/

- Gmcdouga. (2024a, October 17). A closer look at Q3 2024: 75% surge in cyber attacks worldwide. Check Point Blog. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/#:~:text=A%20Record%20Spike%20in%20Attacks,rise%20from%20the%20previous%20quarter.

- Hall, C. (2023, Feb 01). U-M health websites attacked. Livingston County Daily Press & Argus Retrieved from https://ezaccess.libraries.psu.edu/login?url=https://www.proquest.com/newspapers/u-m-health-websites-attacked/docview/2771236817/se-2

- Haileamlak, A. (2021, November 31). The impact of COVID-19 on health and health systems. National Library of Medicine. https://pmc.ncbi.nlm.nih.gov/articles/PMC8968362/

- Kristen, J. S. (2023, Sep 06). Increase in cyberattacks at hospitals worrisome. Battle Creek Enquirer Retrieved from https://ezaccess.libraries.psu.edu/login?url=https://www.proquest.com/newspapers/increase-cyberattacks-at-hospitals-worrisome/docview/2861047842/se-2

- Li C, Wu Y, Yuan X, et al. Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN. Int J Commun Syst. 2018; 31:e3497. https://doi-org.ezaccess.libraries.psu.edu/10.1002/dac.3497

References (cont.)

- Madanian, S., Chinbat, T., Subasinghage, M., Airehrour, D., Hassandoust, F., & Yongchareon, S. (2024). Health iot threats: Survey of risks and vulnerabilities. Future Internet, 16(11). https://doi.org/10.3390/fi16110389

- Mohsin, A. S. M., & Muyeed, M. A. (2024). IoT based smart emergency response system (SERS) for monitoring vehicles, home, and health status. Discover Internet of Things, 4(1), 22. doi:https://doi.org/10.1007/s43926-024-00073-6

- OVHcloud. (n.d.). How to stop ddos attacks?. OVHcloud. https://us.ovhcloud.com/security/anti-ddos/how-stop-ddos-steps/#:~:text=Once%20an%20attack%20is%20detected,flow%20and%20reach%20the%20server.

- Rojas, A. (2023, Jan 31). University of Iowa hospitals and clinics websites face outages after cyberattack. University Wire Retrieved from https://ezaccess.libraries.psu.edu/login?url=https://www.proquest.com/wire-feeds/university-iowa-hospitals-clinics-websites-face/docview/2771168644/se-2

- Tidy, J. (2023, April 5). KillNet's Targeting of the Health and Public Health Sector (December 2022 – March 2023). U.S. Department of Health and Human Services. https://www.bbc.com/news/technology-67029296

- Tidy, J. (2023, October 6). Ukraine cyber-conflict: Hacking gangs vow to de-escalate. BBC News. https://www.bbc.com/news/technology-67029296

Thanks!