Cyber Security Threat Analysis of Spam

NCI Post Graduate Diploma Cyber Security
Semester 1

Author: Jonathon Taaffe

Title: Cyber Security Threat Analysis of Spam
Author: Jonathon Taaffe

Executive Summary

This *Cyber Security Briefing: The Threat of SPAM* report highlights the statistics, trends, costs and predictions of SPAM relevant to the client.

This report presents detailed intelligence outlining the client's current SPAM position and outlines emerging trends and threats to better manage our exposure.

SPAM: Statistics 2018

Global Context: 289.71 Billion SPAM emails sent globally every day.[1]

Client Context: 3 Million SPAM emails addresses to @client.domain in 2018; 100 SPAM emails per employee per day.

SPAM Email Detection:

- 2.94 Million (98%) SPAM emails rejected at external Check Point Firewalls.
- 60K (2%) SPAM emails evaded first line of defence.

Why did 2% of SPAM messages evade our security?

2 Significant Developments:[2]

1. Threat Actors are relying almost entirely on SPAM to deliver their payload because of improvements in Exploit Management and Detection Software:
    a. Decline of Adobe Flash Website Plugins eliminating exploit kits.
    b. Improvements in Anti-Malware detection.

2. Evolution of Threat Actors Social Engineering Skills
    a. SPAM emails with error-free subject lines and content.
    b. SPAM emails with image-based content rather than text-based content.
    c. SPAM email sender address that 'appears' to resemble a valid, business related email address or a known contact of the recipient.

    Delivered SPAM content included:

    - 46% Dating Scams
    - 31% Emails with Malicious Website Links
    - 23% Emails with Malicious Attachments
        - 85% of Malicious Attachments: .ZIP .DOC .XLS .PDF .7Z

Important Note: Of the 2% delivered, 100% of Malicious SPAM payloads were either blocked or stripped by second line of defence; Malicious Website Filtering and/or Malicious Email Attachment Stripping.

---

[1] Cisco Talos Intelligence Group (2019) *Email and Spam Data || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence.* Available at: https://www.talosintelligence.com/reputation_center/email_rep [Accessed 11 Feb. 2019].
[2] F-Secure (2018) *Why spam is on the rise – again*. Available at: https://blog.f-secure.com/why-spam-is-on-the-rise-again/ [Accessed 10 Feb. 2019].

SPAM: Trends

1. Malicious SPAM (MalSPAM) volumes significantly increased through 2018 through Threat Actor use of the Necurs Botnet.

    - Bot: software that executes simple repetitive automated tasks.
    - Botnet: a network of internet connected devices running Bot software.
    - Necurs: name of a Botnet which distributes MalSPAM.

    In 2018 from September 11th to September 19th, 4.95 Billion MalSPAM emails were sent from the Necurs Botnet alone.[3]

2. In the Financial Sector, the Emotet Trojan accounted for 76% of all Trojans in 2018.[4]

    > "*Emotet is an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Additionally, Emotet is a polymorphic banking Trojan that can evade typical signature-based detection.*"[5]

    Emotet is delivered through MalSPAM (Malicious SPAM) that is designed using familiar branding including PayPal receipts and Amazon Shipping Notifications.

    As of publication, the client has not been impacted with Emotet, but awareness is key.

3. Through 2018 SPAM content evolved to target Multi-Language Audiences.[6] This was reported at our European office where previously English-only SPAM was received but this year German language SPAM was circulated.

4. Emergence of Business E-Mail Compromise (BEC) exploits.[7]

    A Threat Actor creates an email address which looks almost identical to a valid email account. Using this 'spoofed' email address, the Threat Actor sends emails to valid corporate email accounts with the intent to defraud.

    Examples of spoofed and valid client corporate email addresses:

John.Doe@client.domain (spoofed)	Jon.Doe@client.domain (valid)
Alice.Othere@client.domain (spoofed)	Alice.Other@client.domain (valid)

    As demonstrated, by adding an additional letter or changing a letter, a 'spoofed' email address can appear to be valid.

---

[3] Sowells, J. Hacker Combat Community (2018*) Necurs Botnet's New Scamming Spam Emails*. Available at: https://hackercombat.com/necurs-botnets-new-scamming-spam-emails/ [Accessed 13 Feb. 2019]

[4] ProofPoint. (2019) *Threat Actor Profile: TA505, from Dridex to GlobeImposter*. Available at: https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter/ [Accessed 9 Feb. 2019]

[5] Department of Homeland Security (2018) *CISA | Cyber + Infrastructure | Alert (TA18-201A) - Emotet Malware*. Available at: https://www.us-cert.gov/ncas/alerts/TA18-201A [Accessed 14 Feb. 2019]

[6] Vergelis, M., Demidova, N. and Shcherbakova, T. Secure List (2018) *Spam and phishing in Q3 2018*. Available at: https://securelist.com/spam-and-phishing-in-q3-2018/88686/ [Accessed 9 Feb. 2019]

[7] Federal Bureau of Investigation (2017) *Business E-Mail Compromise | Cyber-Enabled Financial Fraud on the Rise Globally*. Available at: https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise [Accessed 10 Feb. 2019]

SPAM: Costs

SPAM Email Volume Breakdown for 2018

Detail	Result	Calculation
SPAM Emails Delivered (total)	60,000	
SPAM Emails per Employee per Year	750	(60,000/80 employees)
SPAM Emails per Employee per Day	3	(250 working days)

Employee Time Lost Addressing SPAM Email

Detail	Result	Calculation
Per Employee per day	90 seconds*	(3 SPAM emails x 15 seconds)
All Employees per day	2 hours	(90 seconds x 80 employees)
All Employees per week	10 hours	(600 minutes)
All Employees per year	500 hours	(50 weeks)

* Average time to address a single SPAM email: 30 seconds

Client Annual SPAM Costs

Details	Result	Calculation
Productivity Loss	€12,500	(500 hours x €25 per hour*)
IT Storage Costs	€ 8,500	
Total Annual Cost of SPAM	€21,000	
Total Annual Hours Lost	500 hours	(50 weeks)

*Average annual wage €50,000 (daily: €200, hourly: €25)

Important Notes Regarding Check Point Firewall Costs

i. The above Total Annual Cost of SPAM does not include annual Check Point Firewall Direct Enterprise Support (Premium) Running Cost of €65,000.
ii. Check Point Firewall Running Costs include Licensing, Servicing, Support and Maintenance costs.
iii. Servicing Costs include 24x7 Firewall Rule and Filter updates for SPAM, Malicious Website URL's and Anti-Malware Signatures. [8]

SPAM: Predictions

- Continued Year on Year growth of Malicious SPAM (MalSPAM) volumes globally.
- Increase in Business E-Mail Compromise (BEC) exploits.[9]
- Further development of Threat Actors Social Engineering Skills.
- Evolution of Geolocation specific SPAM email.[10]

[8] Check Point (2019) *Support Plans.* Available at: https://www.checkpoint.com/support-services/support-plans/ [Accessed 15 Feb. 2019]
[9] ZDNet.com. (2019) *Cybercrime and malware, 2019 predictions*. Available at: https://www.zdnet.com/pictures/cybercrime-and-malware-2019-predictions/9/ [Accessed 15 Feb. 2019]
[10] Kabel, H. (2019) *Fraud Predictions: What's in Store for 2019?* Available at: https://blog.easysol.net/fraud-predictions-2019/ [Accessed 15 Feb. 2019].

References

1	Cisco Talos Intelligence Group	(2019)	Email and Spam Data || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence.	https://www.talosintelligence.com/reputation_center/email_rep	[Accessed 11 Feb. 2019].
2	F-Secure	(2018)	Why spam is on the rise – again.	https://blog.f-secure.com/why-spam-is-on-the-rise-again/	[Accessed 10 Feb. 2019].
3	Sowells, J. Hacker Combat Community	(2018)	Necurs Botnet's New Scamming Spam Emails.	https://hackercombat.com/necurs-botnets-new-scamming-spam-emails/	[Accessed 13 Feb. 2019]
4	ProofPoint.	(2019)	Threat Actor Profile: TA505, from Dridex to GlobeImposter.	https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter/	[Accessed 9 Feb. 2019]
5	Department of Homeland Security	(2018)	CISA | Cyber + Infrastructure | Alert (TA18-201A) - Emotet Malware.	https://www.us-cert.gov/ncas/alerts/TA18-201A	[Accessed 14 Feb. 2019]
6	Vergelis, M., Demidova, N. and Shcherbakova, T. Secure List	(2018)	Spam and phishing in Q3 2018.	https://securelist.com/spam-and-phishing-in-q3-2018/88686/	[Accessed 9 Feb. 2019]
7	Federal Bureau of Investigation	(2017)	Business E-Mail Compromise | Cyber-Enabled Financial Fraud on the Rise Globally.	https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise	[Accessed 10 Feb. 2019]
8	Check Point	(2019)	Support Plans.	https://www.checkpoint.com/support-services/support-plans/	[Accessed 15 Feb. 2019]
9	ZDNet.com.	(2019)	Cybercrime and malware, 2019 predictions.	https://www.zdnet.com/pictures/cybercrime-and-malware-2019-predictions/9/	[Accessed 15 Feb. 2019]
10	Kabel, H.	(2019)	Fraud Predictions: What's in Store for 2019?	https://blog.easysol.net/fraud-predictions-2019/	[Accessed 15 Feb. 2019]