
CYLANCE
2019
THREAT
REPORT
DISCUSSION GUIDE

# Reader Interest Summary

The Cylance® 2019 Threat Report provides unique findings drawn from our consulting engagements, threat research and intelligence efforts, and through feedback provided by Cylance customers. Highlights of the 2019 edition of our threat report include the following key findings:

- Non-profits, the food industry, and the logistics sector reported the greatest number of cyber attacks in 2018
- Coinminer detections increased by 47%
- The top five threats reported by Cylance OS X clients
- APTs deploying a novel loader using steganography to read payloads hidden in .PNG files
- How behavioral-based AI security solutions may have prevented recent successful attacks
- Cybersecurity predictions for 2019

The Cylance 2019 Threat Report features analysis on the top threats to impact Cylance customers using both Windows and OS X systems, and a wealth of longer-form topics including APT trends, cybersecurity insights, year-over-year analysis, consumer sentiment, and more. Most importantly, the Cylance 2019 Threat Report provides Cylance's unique piece of the larger cybersecurity picture and details you cannot glean from other sources.

# Topics For Discussion

Several topics in the Cylance 2019 Threat Report invite further discussion on critical cybersecurity issues. Exploring these subjects with peers and colleagues may offer new insight into the current state of your security posture, areas for improvement, and unconventional approaches that could save your organization time and money.

We encourage you to use the following discussion topics to guide discussions with your team about how you can best protect your organization in 2019 and beyond:

1. ***Report Finding:*** *"In 2018, coinminer detections increased by 47%."*

   **Questions:**

   - How do coinminers operate and how can you detect their presence in your infrastructure?
   - What is fueling their rapid growth?

   **For Consideration:** The rise of coinminers can largely be attributed to simple market forces. For cyber criminals motivated by profit, coinminers offer a surreptitious alternative to ransomware. Coinminers, as the name suggests, use processing resources to perform the complex calculations required to unlock cryptocurrencies like Bitcoin. Threat actors who deploy coinminers to target systems can reap the financial rewards of cryptocurrencies without announcing their presence to victims. Coinminers provide a superior alternative to ransomware by providing reliable rewards without requiring the consent or compliance of victims.

   Coinminers require considerable processing power and therefore produce a noticeable strain on central processing unit (CPU) and graphical processing unit (GPU) resources. A consistently heavy workload persisting on CPU/GPU resources or an overall degradation of system performance may indicate the presence of a coinminer infection. Coinminers often arrive as email attachments and are installed via drive-by downloads.

2. ***Report Finding:*** *"In 2018, Cylance saw an increase in phishing attacks, most of them focused on Microsoft Office 365 (O365) credential harvesting."*

   **Questions:**

   - Is your organization vulnerable to this or any other type of credential harvesting?
   - What kind of dangers do stolen credentials represent to your business?

   **For Consideration:** Cylance observed attackers exploiting stolen O365 credentials in numerous ways during 2018. Successful attackers set up email inbox forwarding rules to control the information of compromised users. Emails containing phrases of interest were redirected to threat actors for further analysis. Emails containing notifications of account modifications were removed from the inbox before a compromised user discovered them.

   By controlling the information flow of user email boxes, attackers can successfully execute direct deposit modifications and man-in-the-middle attacks on wire transfers. Another popular target of cyber criminals is intellectual property that can be sold or used for the benefit of threat actors. Since legitimate credentials are used to make the various account modifications required for these attacks, the malicious activity may go undetected until financial losses occur.

   User credentials are most often harvested through phishing campaigns. There are several preventative steps organizations can take to protect themselves from these attacks. Enabling mailbox audit logging, blocking email forwarding rules, and requiring multi-factor authentication (MFA) for all users are good first steps.

3. ***Report Finding:*** *"If there is one threat that dominated 2018 in terms of propagation and persistence, it is Emotet. The Emotet of 2018 is a vastly different creature from the original 2014 version. It has evolved from a banking trojan into a robust and multi-faceted threat tool."*

   **Questions:**

   - How are cyber threats like Emotet evolving?
   - What do these more complex and multi-faceted threats mean in terms of how your organizations should prepare to protect itself?

**For Consideration:** Emotet first appeared as a simple banking trojan in 2014. Since then, it has received numerous upgrades that have transformed it into a modular attack platform. The threat actors behind Emotet have implemented analysis awareness, multi-layered C2 encryption, brute-force credential attacks, and full-body email harvesting into the malware. Emotet can also leverage DKIM controls to bypass spam controls, use PDFs to trigger malicious links, and download additional instructions from C2 servers.

The expansion of Emotet's capabilities made it a major delivery platform for threats like IcedID, Trickbot, Qakbot, and other malware. Emotet is polymorphic, and the Emotet platform uses a dynamic infrastructure that regularly updates malicious documents and rotates encryption keys. Emotet can exfiltrate the full body of emails, which provides attackers valuable intelligence for increasing the success rate of future phishing campaigns.

One effective response to evolving threats like Emotet is using a prevention-based security solution. For example, Cylance's endpoint protection product, CylancePROTECT®, uses cloud-trained AI security agents to detect and prevent polymorphic and zero-day malware. Prevention is achieved by identifying the feature profile of threats during pre-execution instead of searching for specific and previously identified malware files.

4. ***Report Finding:*** *"For perspective on credential-based attacks, The Register[1] reports that attackers trying to crack user accounts may generate 90% of online retail traffic. Given the frequency of credential-based attacks, it is unsurprising that cyber criminals landed so many large attacks in 2018."*

   **Questions:**

   - How can your organization prevent credential-based attacks?
   - How can your organization detect successful credential-based attacks?

   **For Consideration:** Credential-based attacks occur when threat actors acquire legitimate credentials for accessing target systems. Legitimate credentials are often collected through phishing emails, though some malware can also harvest user login information. Resourceful attackers may scour employees' social media, or pose as co-workers on sites like LinkedIn, hoping to uncover information useful for stealing credentials.

   Preventing credential-based attacks is often as simple as training employees to identify and avoid common credential-harvesting tactics. Ensure employees understand how to identify and avoid phishing emails. Educate employees on the dangers of over-sharing job-related material on social media or exposing information that may assist with credential theft.

   Once legitimate credentials are compromised, detecting a credential-based attack becomes difficult. Analysts and outside observers will have very little indication that anything is amiss when attackers appear as legitimate users within the environment. Requiring multi-factor authentication, segmenting the environment, and maintaining strict user access control may limit the damage a compromised account can inflict. Another remedy to credential-based attacks may be implementing AI-driven behavioral analysis. Tactics like credential hijacking and malicious service account activity can be quickly detected by AI trained to identify anomalous behavior. When potentially dangerous system behavior is detected, early mitigation steps can be initiated before real damage occurs.

[1] ps://www.theregister.co.uk/2018/07/20/credentials_login_slurp

**Want to learn more about what an AI-driven, prevention-based approach to endpoint security could do for you? We've got you covered at cylance.com**

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

CYLANCE



20190228-0145