CYLANCE

2017 THREAT REPORT

DISCUSSION GUIDE

READER INTEREST SUMMARY

The Cylance 2017 Threat Report offers valuable analysis on the current state of cybersecurity. The information provided in the report is unavailable anywhere else. This Cylance® study includes research and information drawn from internal data and feedback provided by Cylance customers. The report offers considerable insights into recent threat trends and related security issues. Highlights include:

- Cylance prevented over 3,900 unique attacks per enterprise across more than 160 countries — **an increase of over 13% in the amount of attacks** seen within the Cylance ecosystem in 2016
- Ransomware attacks affected all verticals, but **impacted healthcare the most**
- Many of the attacks in 2017 were initiated by **exploiting vulnerabilities reported more than nine months prior to the attack**
- The **top two infection vectors remained email and drive-by downloads**

The report explores the exponential growth of cyberthreats, a result of the continued rise in targeted attacks utilizing unique, single-use malware. Within the Cylance community, **more than 70% of the threats blocked were never detected by anyone else.**

The report also contains an analysis of the top 10 malware threat families. Malware heavyweights WannaCry, Upatre, Cerber, Emotet, Locky, Petya, Ramnit, Fareit, Polyransom, and Terdot/Zloader each receive an individual study. Also included is Cylance's prediction that threat actors intend to continue leveraging firmware and hardware vulnerabilities into persistence mechanisms and future breach points.

TOPICS FOR DISCUSSION

Some key findings of this report merit further discussion. These conversations represent an opportunity to dig deeper into the implications of current security strategy and its ability to protect against future threats. We invite you to use the following as a guide to explore some of these topics of conversation further with your peers:

1. "More than 70% of the threats Cylance blocked were never detected by anyone else."

   Where did these unique threats originate, and why did other AV solutions fail to detect them?

   The rise of single-use malware and ransomware-as-a-service (RaaS) has enabled the automated generation of massive numbers of unique threats. Attackers are now using machine learning to generate high volumes of threats, resulting in greater overall efficacy against signature-based AV products.

   During private tests performed by SE Labs, CylancePROTECT was subjected to new and unique variations of real-world malware. Cylance detected and prevented the lab-generated variations with an average of 25 months of predictive advantage. **Is your endpoint security set up and optimized to protect against the massive tide of both known and unknown threats?**

2. "Many of the attacks in 2017 were initiated by exploiting vulnerabilities that were reported more than nine months before the attack was detected and blocked."

   This detail invites discussion on the importance of keeping the environment updated.

   AI driven prevention models can alleviate the need for the continuous updating required by traditional solutions. **How is your organization keeping up with critical updates to ensure you're protected against threats now and into the future? How many resources are consumed in the process of performing these regular updates?**

3. "The top two infection vectors remained email and drive-by downloads."

   How much training and education is required to get employees informed about the top threat vectors and malware indicators so that the human element is reduced as a component of an organizations' overall vulnerability? **Is there any way to automate the security judgment call so that one click on one email can't bring down your entire business?**

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 WWW.CYLANCE.COM

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
400 Spectrum Center Drive, Irvine, CA 92618

CYLANCE