FireEye Mandiant M-Trends 2020 Report Reveals Cyber Criminals Are Increasingly Turning to Ransomware as a Secondary Source of Income

February 20, 2020

Cyber attacks are evolving – 41% of the malware families FireEye Mandiant observed in 2019 were new

MILPITAS, Calif.--(BUSINESS WIRE)--Feb. 20, 2020-- FireEye, Inc. (NASDAQ: FEYE), the intelligence-led security company, today released the FireEye® Mandiant® M-Trends® 2020 report. The report shares statistics and insights gleaned from FireEye Mandiant investigations around the globe in 2019.

This press release features multimedia. View the full release here: https://www.businesswire.com/news/home/20200220005015/en/

Key findings include:

Organizations Are Detecting and Containing Attacks Faster

In the 2020 M-Trends report, the global median dwell time, defined as the duration between the start of a cyber intrusion and it being identified, was 56 days. This is 28% lower than the 78-day median observed in the previous year. FireEye Mandiant consultants attribute this trend to organizations improving their detection programs, as well as changes in attacker behaviors such as the continued rise in disruptive attacks (e.g. ransomware and cryptocurrency miners) which often have shorter dwell times than other attack types.

Global internal and external detection times have also reduced.

- **Median dwell time for organizations that learned of their incident by an external party:** Stands at 141 days, a 23% decrease since the previous M-Trends report (184 days).
- **Median dwell time for organizations that self-detected their incident:** Stands at 30 days, a 40% decrease year over year (50.5 days). While internal dwell time saw the greatest level of improvement, still 12% of investigations continue to have dwell times of greater than 700 days.

Internal Detection Reaches A Four-year Low

Although the dwell time for intrusions identified internally by organizations has gone down, the overall percentage of self-detected security incidents versus external sources has also reduced. There has been a 12-percentage point decrease in the proportion of compromises detected internally, year-over-year. This comes after a steady increase of internal detections since 2011.

2019 is the first time in four years in which external notifications, when an outside entity informs an organization that it has been compromised, exceeded internal detections.

This shift is potentially due to a variety of factors, such as increases in law enforcement and cyber security vendor notifications, changes in public disclosure norms, and compliance changes. FireEye Mandiant feels it is unlikely that organizations' ability to detect intrusions deteriorated, as other metrics show continued improvements in organizational detections and response.

Hundreds of New Malware Families Identified

The new report details how of all the malware families Mandiant observed in 2019, 41% had never been seen before. Furthermore, 70% of the samples identified belonged to one of the five most frequently seen families, which are based on open source tools with active development. These points demonstrate that not only are malware authors innovating, cyber criminals are also outsourcing tasks to monetize operations faster.

Also of note, the majority of new malware families impacted either Windows or multiple platforms. While FireEye Mandiant saw new malware families solely impacting Linux or Mac, this activity remains in the minority.

Increased Monetization Means More Ransomware Attacks

Of the attacks that FireEye Mandiant professionals responded to, the greatest majority (29%) were likely motivated by direct financial gain. This includes extortion, ransom, card theft, and illicit transfers. The second most common (22%) was data theft likely in support of intellectual property or espionage end goals.

The successful monetization of ransomware attacks and the availability of ransomware as a service have contributed to an increase in overall ransomware cases. Established cybercrime groups that historically targeted personal and credit card information have also been increasingly turning to ransomware as a secondary means of generating revenue. Given the ease with which ransomware attacks can be carried out and their continued financial success for attackers, FireEye expects that ransomware will continue to be used as a secondary means for monetizing access to victim environments.

"FireEye Mandiant has seen organizations largely improving their level of cyber security sophistication, but combatting the latest threats is still a huge challenge for them," said Jurgen Kutscher, Executive Vice President of Service Delivery at FireEye. "There are more active groups now than ever before and we've seen an aggressive expansion of their goals. Consequently, it's crucial for organizations to continue building and testing their defenses."

A full copy of the FireEye Mandiant M-Trends 2020 report is available for download at: https://www.fireeye.com/mtrends

Visit FireEye at RSA

Come discuss these findings and more with FireEye experts at booth N6069 during RSA® Conference 2020 in San Francisco, February 24 – 28. For a full list of where FireEye experts will be speaking throughout the Conference, please visit: https://www.fireeye.com/blog/products-and-services/2020/01/come-see-fireeye-at-rsa-conference-2020.html

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 8,800 customers across 103 countries, including more than 50 percent of the Forbes Global 2000.

View source version on businesswire.com: https://www.businesswire.com/news/home/20200220005015/en/

Source: FireEye, Inc.

Media Inquiries:
Media.Relations@FireEye.com

Investor Inquiries:
Investor.Relations@FireEye.com