elastic security labs

10 takeaways for CISOs from the 2023 Global Threat Report

Built to provide threat insights, the second annual Global Threat Report from Elastic surfaces top findings from months of analysis on more than 1 billion data points, courtesy of private and public telemetry. Elastic Security Labs has categorized these insights into three important buckets: landscape forecasts, adversary tactics, and systems.

Landscape Forecasts

1. Open source tools will become more popular

Open source tools provide threat actors with a free and easy entrance into cybercrime. Elastic observed several open source malware tools both in our Global Threat Report analysis and in research that pre-dates our findings here, like the r77 rootkit and JOKERSPY.

2. There will be more malware-as-a-service (MaaS) for newer threat actors

Adversaries are utilizing the as-a-service (AaS) model to fill in knowledge and product gaps as proven by RaaS popularity. Malicious AaS companies will diversify their portfolios to better accommodate buyers, and adversaries utilizing MaaS will rely on the *Obfuscation* and *Masquerading* techniques.

3. Adversaries will tamper with environments more than they hide

As they face increasingly resistant environments, adversaries are more regularly attempting to disable or otherwise tamper with security sensors. Outside of the Global Threat Report analysis, Elastic has also observed an increase in attacks from OS design flaws like Bring Your Own Vulnerable Driver (BYOVD) to deploy a driver with one or more exploitable weaknesses.

Adversary tactics

4. Ransomware is expanding and diversifying

Between high-profile examples like WannaCry and NotPetya, ransomware has proven a potent threat over the years. Ransomware-as-a-service (RaaS) campaigns accounted for 81% of all ransomware observed, likely due to a lower barrier to entry for both new and veteran adversaries. We can expect threat actors to further innovate in this category.

5. Adversaries are comfortable navigating through systems

Almost half (43.89%) of observed endpoint behavior fell under *Defense Evasion*. The significance of this number suggests that adversaries are familiar with, and feel comfortable, evading security systems.

6. Malicious code is being executed through built-in OS utilities

Elastic observed that 48% of *Defense Evasion* techniques run on endpoints were methods of *System Binary Proxy Execution*, which allows threat actors to run malicious code within a native OS program. The popularity of this technique may come from how time-consuming it is to analyze these types of alerts.

7. Adversaries rely on *Credential Access* techniques in Cloud environments

Elastic observed an 11% increase in *Credential Access* signals, indicating that credentials have become an essential part of the cloud intrusion process. This could signify ease of credential gathering, or imply that environments lack the visibility necessary to identify when valid credentials are being used fraudulently.

Systems

8. Greater Windows observability revealed Azure popularity

Elastic's visibility of Windows environments improved this year, a 422% increase from last year's analysis that includes new visibility into Microsoft 365. In our analysis of cloud service providers, we observed Azure activity rising from 13.14% last year to 36%. While AWS retains that majority, signals from AWS environments have decreased ~10%.

9. While Windows retains the majority of endpoint signals, both macOS and Linux signals have increased notably

94% of endpoint behavior alerts targeted Windows systems, due in part to the increase in Windows-focused telemetry. Overall, Elastic saw significant signal increases for Windows, Linux, and macOS. With an increase of 118%, macOS innovations revealed novel discoveries like RUSTBUCKET.

10. Most observed malware infections were on Linux systems

In the midst of increased observability into all systems from Elastic, Linux still accounted for 91.2% of infections observed. Notably, most of these involved no human intervention and were automated and potentially indiscriminate attacks.

Master the Threat Landscape

Prepare for the evolution of these threats and more. See what the experts at Elastic Security Labs are suggesting in the 2023 Elastic Global Threat Report. Follow Elastic Security Labs on X (formerly Twitter) @ElasticSecLabs and check out our articles for the latest threat developments, research, and more!

