elastic security labs

Zehn Erkenntnisse für CISOs aus dem Global Threat Report 2023

Der zweite jährliche Global Threat Report von Elastic liefert Bedrohungsinformationen und fördert wichtige Erkenntnisse aus monatelangen Analysen von mehr als einer Milliarde Datenpunkten aus privaten und öffentlichen Telemetriedaten zutage. Elastic Security Labs hat diese Erkenntnisse in drei wichtige Kategorien unterteilt: allgemeine Prognosen, Angreifertaktiken und Systeme.

Allgemeine Prognosen

1. Open-Source-Tools werden immer beliebter
Open-Source-Tools bieten Angreifern einen kostenlosen und einfachen Einstieg in die Welt des Cyberverbrechens. Elastic hat verschiedene Open-Source-Malware-Tools in der Analyse zum Global Threat Report und bei vorherigen Forschungen gefunden, wie etwa das r77-Rootkit und JOKERSPY.

2. Neuere Angreifer werden immer häufiger Malware-as-a-Service (MaaS) einsetzen
An der Beliebtheit von RaaS ist erkennbar, dass Angreifer das as-a-Service-Modell (AaS) nutzen, um Wissens- und Produktlücken zu schließen. Bösartige AaS-Unternehmen werden ihre Portfolios erweitern, um Käufern entgegenzukommen, und Angreifer werden MaaS in Kombination mit *Verschleierungs-* und *Maskierungstechniken* nutzen.

3. Angreifer werden Umgebungen zunehmend manipulieren, anstatt sich zu verstecken
Angesichts zunehmend widerstandsfähiger Umgebungen versuchen Angreifer immer häufiger, Sicherheitssensoren zu deaktivieren oder anderweitig zu manipulieren. Außerhalb der Analysen für den Global Threat Report hat Elastic außerdem eine Zunahme an Angriffen auf Basis von BS-Designlücken wie etwa Bring Your Own Vulnerable Driver (BYOVD) beobachtet, bei denen ein Treiber mit einer oder mehreren ausnutzbaren Schwachstellen eingesetzt wird.

Angreifertaktiken

4. Ransomware wird immer umfangreicher und vielfältiger
Mit prominenten Beispielen wie WannaCry und NotPetya hat sich Ransomware im Lauf der Jahre als ernstzunehmende Bedrohung erwiesen. Ransomware-as-a-Service-Kampagnen (RaaS) waren für 81 % aller beobachteten Ransomware verantwortlich, vermutlich aufgrund der niedrigen Einstiegshürde für neue und erfahrene Angreifer gleichermaßen. In dieser Kategorie erwarten wir weitere Innovationen von Angreifern.

5. Angreifer navigieren zielsicher durch Systeme

Beinahe die Hälfte (43,89 %) der beobachteten Endpoint-Verhaltensweisen fiel in die Kategorie *Tarnung*. Dieser hohe Wert legt nahe, dass die Angreifer mit den Sicherheitssystemen vertraut sind und diese zielsicher umgehen.

6. Schadcode wird mithilfe von integrierten BS-Hilfsprogrammen ausgeführt

Elastic hat festgestellt, dass 48 % der auf Endpoints ausgeführten *Tarnungstechniken* eine Art von *System Binary Proxy Execution* verwendeten, mit der die Angreifer Schadcode innerhalb von nativen Betriebssystemprogrammen ausführen konnten. Diese Technik ist auch daher sehr beliebt, weil es unglaublich zeitraubend ist, die entsprechenden Warnungen zu analysieren.

7. Angreifer nutzen Zugriffe mit *Anmeldeinformation* in Cloud-Umgebungen

Elastic hat einen Anstieg von 11 % bei den Signalen für Zugriffe mit Anmeldeinformation beobachtet. Dies deutet darauf hin, dass diese Art von Cloud-Angriffen immer häufiger eingesetzt wird. Möglicherweise ist es einfach, *Anmeldeinformationen* zu sammeln, oder die Umgebungen sind nicht transparent genug, um erkennen zu können, ob gültige Anmeldeinformationen auf betrügerische Weise genutzt werden.

Systeme

8. Zunehmende Windows-Observability zeigt die Beliebtheit von Azure

Die Elastic-Einblicke in Windows-Umgebungen haben im Vergleich zur letztjährigen Analyse um 422 % zugenommen und liefern neue Einblicke in Microsoft 365. Bei unserer Analyse der Cloud-Dienstanbieter hat die Azure-Aktivität von 13,14 % auf 36 % zugenommen. AWS ist zwar weiterhin Marktführer, aber die Signale aus AWS-Umgebungen haben um etwa 10 % abgenommen.

9. Windows liefert weiterhin die meisten Endpoint-Signale, aber macOS und Linux haben deutlich zugenommen

94 % der Endpoint-Verhaltenswarnungen bezogen sich auf Windows-Systeme, teils auch durch die Zunahme an Windows-spezifischer Telemetrie. Insgesamt verzeichnete Elastic deutliche Signalzunahmen für Windows, Linux und macOS. Mit einem Anstieg von 118 % haben macOS-Innovationen neue Erkenntnisse wie RUSTBUCKET zutage gefördert.

10. Die meisten Malware-Infektionen wurden auf Linux-Systemen beobachtet

Inmitten der zunehmenden Elastic-Observability in allen Systemen wurden weiterhin 91,2 % Infektionen auf Linux-Systemen beobachtet. Die meisten dieser Angriffe erfolgten automatisch ohne menschliches Eingreifen, und es handelte sich um potenziell wahllose Angriffe.

Bedrohungslandschaft beherrschen

Machen Sie sich bereit für die Weiterentwicklung dieser und anderer Bedrohungen. Lesen Sie die Empfehlungen der Experten der Elastic Security Labs im Elastic Global Threat Report 2023. Folgen Sie den Elastic Security Labs auf X (ehemals Twitter) @ElasticSecLabs und lesen Sie unsere Artikel über die neuesten Bedrohungsentwicklungen, Forschungsergebnisse und vieles mehr!

