DAS PROJEKT ELDERWOOD

Das Team von **Symantec Security Response** hat eine **weltumspannende IT-Infrastruktur** entdeckt, über die **global zahlreiche gezielte Cyberangriffe** gegen mehrere Organisationen abgewickelt wurden.

8
Zero-Day-Schwachstellen

- CVE-2010-2049 — 2010
- CVE-2011-0609, CVE-2011-0611, CVE-2011-2110 — 2011
- CVE-2012-0779, CVE-2012-1875, CVE-2012-1889, CVE-2012-1535 — 2012

2
attackierte Anwendungen

- Internet Explorer
- Adobe Flash Player

2
bevorzugte Angriffsmethoden

„Watering Hole"-Attacken

Diese infizieren Webserver und warten dort auf ihre Opfer.

Spear Phishing

Gezielter Versand von E-Mails an wichtige Personen.

Watering Hole vs. Spear Phishing

Sind die Ziele einmal identifiziert, platzieren die Angreifer auf ausgewählten Webseiten, welche die Zielpersonen wahrscheinlich besuchen werden, digitale Fallen.

Diese Angriffstechnik...

- setzt Know-how und Zielstrebigkeit voraus, um den Exploit auf einer geeigneten Webseite zu platzieren
- ist effektiv, es kann jedoch einige Zeit vergehen, bis das Opfer die „Wasserstelle" besucht
- verspricht eine große Zahl von Opfern und gestohlenen Daten
- verursacht mehr Kollateralschäden

Die identifizierten Ziele erhalten E-Mails mit einem Anhang oder einem Link, den sie öffnen beziehungsweise anklicken sollen.

Diese Angriffstechnik...

- erfordert vergleichsweise wenig Fachkenntnis zur Ausführung
- ist effektiv, wobei E-Mails anfällig dafür sind, geblockt zu werden
- verspricht eine kleinere Zahl an Opfern und gestohlenen Daten
- verursacht aufgrund des Einsatzes gezielter E-Mails weniger Kollateralschäden

Angriffsziele

Vorrangiges Ziel ist der Verteidigungssektor inklusive seiner Zulieferer

Weitere Ziele werden als Steigbügel genutzt, um an die eigentlichen Ziele zu gelangen

- Verteidigung
- NGO
- Finanzsektor
- Software-branche
- Schifffahrt
- Luftfahrt
- Rüstung
- Energie
- Produktion
- Konstruktion
- Elektroindustrie

Motive

Was sind die Beweggründe dieser Angriffe?

- geistiges Eigentum
- Geschäftsgeheimnisse und Designs
- Pläne
- Kontaktdetails
- Details zur Infrastruktur
- Informationen zur Vorbereitung weiterer Angriffe

Wer

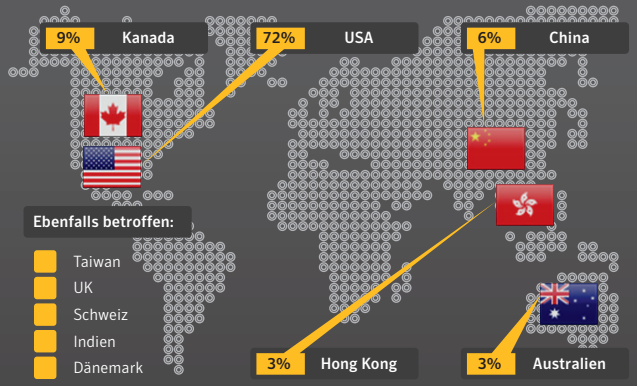
sind die möglichen Angreifer?

Jede dieser Gruppen könnte hinter den Angriffen stecken:

- eine große und finanziell gut ausgestattete kriminelle Gruppierung
- eine von einem Staat unterstützte Gruppierung
- ein Staat

Weltweite Verbreitung

Die Top-5-Länder mit den meisten Malware-Infektionen, die auf Elderwood zurückgehen



Schutzmöglichkeiten

Antivirus (Files)

x 19

- Backdoor.Briba
- Backdoor.Vasport
- Trojan.Naid
- Viele mehr...

Intrusion Prevention (Netzwerk)

x 12

Weitere Schutzmechanismen

- **Reputation**: Norton SafeWeb, Insight Protection
- **Symantec.Cloud**: Symantec MessageLabs E-Mail Security.Cloud
- **SONAR**: Bloodhound.SONAR

Quellen

http://www.symantec.com/security_response/whitepapers.jsp
http://www.symantec.com/security_response

Symantec™ Security Response