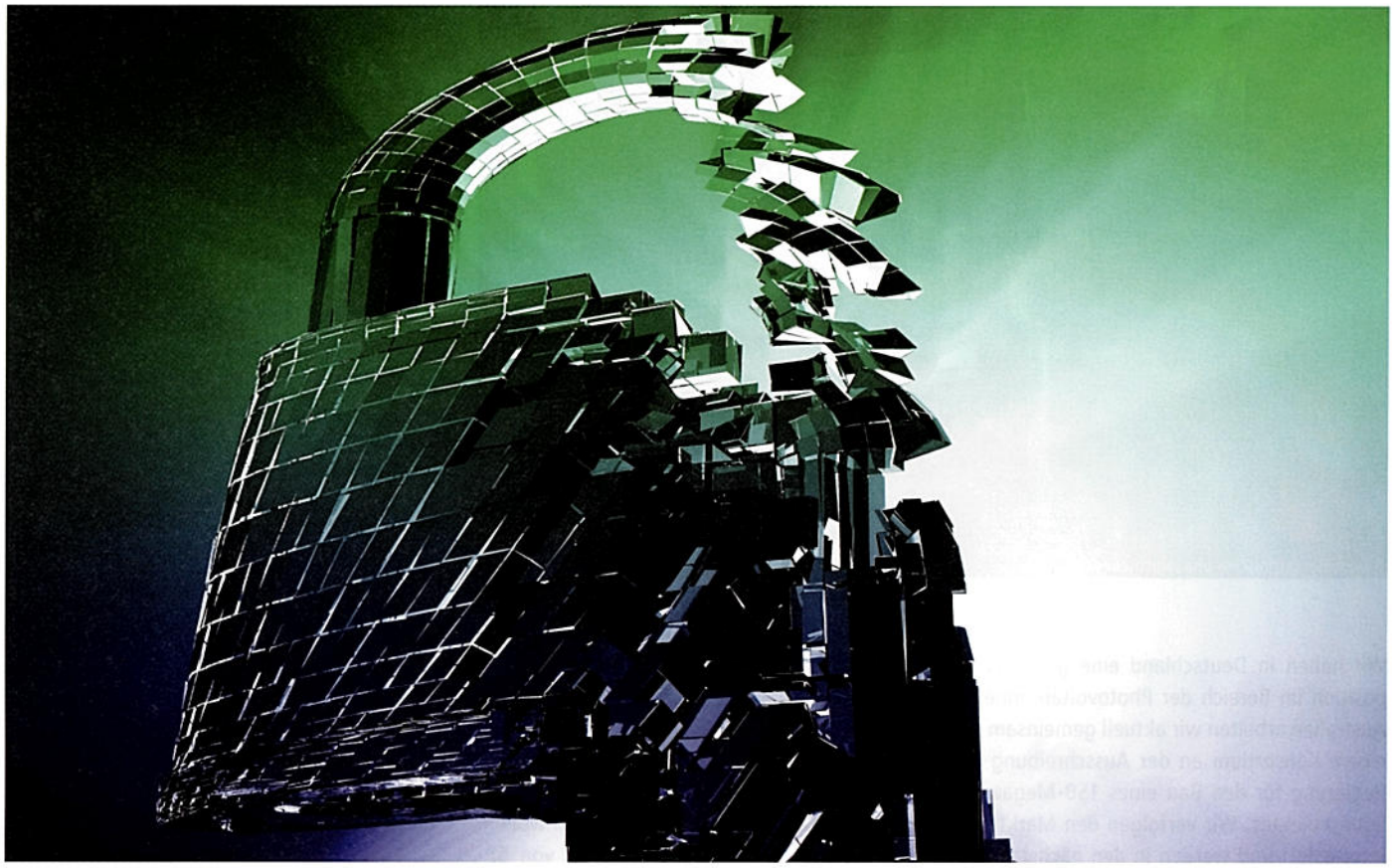

Cyber-Kriminalität macht keine Ferien

DIE TOP FIVE SECURITY- UND THREAT-TRENDS FÜR DEN SOMMER

von Franz Kaiser

Trotz verstärkter, weltweiter Zusammenarbeit der Behörden im Kampf gegen das organisierte Internetverbrechen ist auch in den kommenden Monaten keine Entspannung der Bedrohungslage in Sicht. Es ist weiterhin mit einer Zunahme der 64-Bit-Angriffe und einer steigenden Nachfrage nach Entwicklern sowie kriminellen Dienstleistungen zu rechnen. Dank Source-Code Recycling werden immer mehr Kriminelle versuchen, im Cyberspace leichtes Geld zu verdienen.

Bereits im letzten Jahr haben sich mehrere Länder erfolgreich im Kampf gegen Cyber-Kriminalität zusammengeschlossen. Allerdings wurden eher kurzfristige Erfolge erzielt, da nur die offensichtlichsten Rechtsverstösse verfolgt wurden. Nachdem beispielsweise das riesige Koobface-Botnet von den Behörden zerschlagen wurde, dauerte es nur eine Woche, bis es mit voller Leistung wieder online war. Daher werden Behörden auch weiterhin weltweit ihre Zusammenarbeit ausbauen und verstärkt mit Security Task Forces zusammenarbeiten, um die wachsende Zahl krimineller Aktivitäten im Internet einzudämmen. Die Ausschaltung des Zeus-Botnets 2010 mit zahlreichen Anklagen in den USA und Grossbritannien belegt erste Erfolge.

Vermehrung infizierter Maschinen

Zwischen Internetkriminellen herrscht aktuell ein Verteilungskampf, da kontrollierte Infektionen längere Uptimes der Maschinen und höhere Einnahmen für die Betreiber bedeuten. Daher werden sogenannte Bot-Killer auf Maschinen geschleust, die vorhandene Schadsoftware der Konkurrenz beseitigen. Der Wert der bereits infizierten Geräte wird weiter steigen, wodurch kriminelle Dienstleistungen an Bedeutung gewinnen. Dazu zählen beispielsweise die Bot-Vermietung zur Streuung von Schadsoftware und die Verbreitung von Programmen zur Steigerung der Uptime einer infizierten Maschine.

Damit Infektionen unbemerkt bleiben, werden sich Malware-Betreiber verstärkt der «Qua-

litätssicherung» zuwenden. Entsprechende Dienstleister sorgen für reibungslose Operationen, indem sie beispielsweise eine Software blockieren, die Rechner zum Absturz bringt oder die kriminellen Machenschaften anderweitig behindert. Darüber wird das Leasing von Infektionszeit eine grössere Rolle spielen. Immerhin ein Vorteil: Die Malware beseitigt sich nach Ablauf der Periode selbst vom infizierten Rechner.

Von der 32- zur 64-Bit-Infizierung

Technologien wie Adress Space Layout Randomization (ASLR), Data Execution Prevention (DEP), Virtualisierung und Sandboxing gehören mittlerweile genauso zum Standard wie 64-Bit-Rechner. Diese Entwicklung hat zwar die Verbreitung von Malware verlangsamt, doch nicht aufgehalten. Fortinet geht davon aus, dass auch im Sommer fieberhaft an der Beseitigung existierender Hindernisse gearbeitet wird.

Schon 2010 wurden ASLR- und DEP-Technologien mithilfe von PDF/Flash-Exploits überwunden, und das 64-Bit-Rootkit Alureon hebelte den Vista-Kernelschutz PatchGuard aus. Aktuell ist mit weiteren 64-Bit-Rootkits sowie innovativen Angriffen zur Überwindung von ASLR/DEP und Sandboxing zu rechnen.

Cyber-Kriminelle akquirieren

Da aktuell nicht zuletzt durch konzertierte Aktionen der Behörden «Personal» aus dem Verkehr gezogen wird, müssen die Lücken schnell wieder gefüllt werden. Entwickler für Custom-Packer-Software und -Plattformen, Hosting-Dienste, CAPTCHA-Breaker und Anti-Erkennung sowie Distributoren von Schadcodes sind gefragt. Der grösste Bedarf wird im Bereich Distribution erwartet, da für die Verbreitung von Malware besonders viele Komplizen benötigt werden. Bislang bauten Betreiber ihre Bot-Netze noch selbst auf. Heute überlassen immer mehr Betreiber diese Aufgabe bezahlten Mittelsmännern.

Quellcode-Recycling

Malware tritt in den verschiedensten Erscheinungsformen auf. Die diversen Informationen der Security-Anbieter zu aktuellen Bedrohungen verstärken die allgemeine Verwirrung jedoch nur, anstatt sie zu beseitigen. Die Ursache hierfür ist die steigende Zahl an Malware-Entwicklern, die mit bereits verfügbaren, «geliehenen» Quellcodes und Quellcode-Sammlungen arbeiten. Auch in den kommenden Monaten ist mit einem Zuwachs an Cyber-Kriminellen zu rechnen, die mit wiederverwerteten Quellcodes Geld verdienen wollen. Schon jetzt sind zahlreiche Malware-Programme nahezu identisch, was auf die Nutzung des gleichen Quellcodes durch die Entwickler schliessen lässt. Im März 2011 registrierte Fortinet beispielsweise eine neue Version des Torpig Bot-Netzes, welches für über 35 Prozent der gesamten Bot-Netz-Aktivität verantwortlich ist und damit aktuell auf Platz eins liegt. Torpig ist bereits seit längerem bekannt und erfreut sich nun einer «Wiederauflage».

Während öffentliche Quellcodes weiterhin Probleme in der Security-Landschaft verursachen, steigt sowohl der Wert privater Quellcodes als auch die Bedeutung von Nachwuchsentwicklern. Daher erwartet Fortinet neue Fälle von undichten privaten Quellen, die von neuen Senkrechtstartern genutzt werden, um den Teufelskreis weiterzuführen.

Weitere Informationen

Franz Kaiser
ist Country Manager Austria, Switzerland and Central Eastern Europe, Fortinet.

www.fortinet.ch