Gozi, Tinba, Bladabindi oder:
Die Welt(karte) der Malware 2015

SophosLabs zeigen auf, wo auf der Welt in diesem Jahr welche Schadsoftware besonders stark vertreten war

Wiesbaden, 25. November 2015 So unterschiedlich wie die Kulturen, die Sprachen oder die Küchen auf den Kontinenten unserer Welt, so unterschiedlich sind interessanterweise auch die bevorzugten IT-Schädlinge. Die Sicherheitsexperten bei Sophos Labs haben in einer exklusiven Erhebung anhand von eigenen, vorliegenden Daten nachvollzogen, welche Schadsoftware wo auf der Welt im Jahre 2015 besonders ihr Unwesen trieb.

Was die DACH-Region betrifft, ist dies übrigens sehr eindeutig: die Cyberkriminellen zielten auf Finanzen. Banking Trojaner waren die häufigste Bedrohung...

Kategorien weltweit
Unterteilt nach Malware-Kategorien waren 2015 die folgende Schädlinge weltweit am stärksten vertreten: Banking Trojaner, erpresserische Ransomware, Download-Software, auf den Diebstahl von Passwörtern ausgelegte Software („Password Stealers“) sowie Spambots.

Innerhalb dieser Kategorien erwiesen sich wiederum die nachfolgend aufgezählten Malwarefamilien als die am häufigsten anzutreffenden:

Bei den Banking Trojanern waren besonders häufig Dridex, Zbot, Dyreza, Vawtrak, Tinba, Qbot, Yebot, Gozi, Emotet, Trustezeb unterwegs.

Für erpresserische Absichten kam Ransomware wie Cryptowall, TorrentLocker, CTBLocker und TeslaCrypt vermehrt zum Einsatz. (Ransomware wird genutzt, um nach unerlaubtem Eindringen und etwa Versperren oder Verschlüsselung der Daten vom Besitzer für deren Wiederfreigabe ein „Lösegeld“ zu fordern.)

Als „Downloaders“, also Software für das ungewollte Herunterladen von Trojanern und anderen Schädlingen wurden weltweit am häufigsten Upatre und Ruckguv genutzt.

Für den unerlaubten Diebstahl von Passwörtern bedienten sich die Hacker rund um den Globus besonders einer Malware namens Fareit. Dieser Password Stealer, so zeigt sich, erfreut sich insbesondere in Europa, Nordamerika und Australien großer Beliebtheit.

Der weltweit beliebteste Spambot für das Überschütten unendlich vieler Rechner mit nervenden Spam-Mails trägt den hübschen Namen Shapouf. Er ist insgesamt weitverbreitet, eine überdurchschnittliche Häufigkeit stellten SophosLabs allerdings für Bangladesch, China, Indien, Singapur und Taiwan fest.

Die Situation auf den Kontinenten in der Übersicht
Auf die Finanzen haben es die Cyberkriminellen vor allem in den reichen Ländern Europas und Nordamerikas abgesehen. Hier hatten Angriffe auf´s Banking durch Trojaner und Ransomware-Erpressungsversuche Hochkonjunktur.

In Südamerika erfolgten Angriffe vor allem durch Spam und Ransomware, zudem fanden sich unerlaubte Systemzugriffe aus der Ferne durch Remote Access Trojaner (RAT).

Letztere sind auch sehr beliebt in Teilen des Mittleren Ostens. Afrika wird ansonsten besonders stark mit Spam belastet, während in Asien neben den „moderneren“ Bedrohungen und dem Evergreen Spam, Würmer und Viren alles andere als ausgedient haben. Australien geht mit einer hohen Anzahl von Bootkits eigene Wege.

Folgendes Bild zeigt sich im Einzelnen auf den Kontinenten

Europa

In Großbritannien waren – nicht sehr überraschend – vor allem Banking Trojaner wie Dridex, Vawtrak, Zbot, Dyreza vorzufinden wobei Dridex mit Abstand am meisten verbreitet ist. Auch Ransomware wie Cryptowall, TorrentLocker, teslacrypt, CTBLocker und die Downloader Upatre und ruckguv gehen verstärkt auf britische Rechner los. Zudem fanden sich in Großritannien eine hohe Zahl an Lnk Würmern sowie Web Schadware (ExpJs and JSRedir).

In Skandinavien kommen am häufigsten Banking Trojaner zum Einsatz. Emotet erweist sich dabei als Spitzenreiter, gefolgt von zbot. Auch erpresserische Ransomware ist im hohen Norden Europas stark vertreten, hier insbesondere durch Cryptowall.

Auch die DACH- Region wurde besonders durch Banking Trojaner bedroht, und auch hier lag emotet ganz weit vorne.

In Italien ist ebenfalls der Geldbeutel das beliebteste Angriffsziel, anders als in den nördlicheren Euro-Ländern kommt hier allerdings der Banking Trojaner Gozi ungewöhnlich häufig zum kriminellen Einsatz, gefolgt von Dridex und Zbot. Zum Eintreiben von Lösegeld steht TorrentLocker als Vertreter der Ransomware ganz oben auf der Liste, ihm folgen Cryptowall und CTBLocker. Auch Passwort Diebstahl ist in Italia verbreitet. Dieser erfolgt mit Fareit.

Was Russland betrifft, so lagen Sophos Labs nur sehr wenige eigene Daten vor, man darf aber mit hoher Wahrscheinlichkeit davon ausgehen, so die Experten, dass auch hier insbesondere Banking Trojaner und erpresserische Ransomware zum Einsatz kommen.

Amerika

Nordamerika
Auch die USA sind ein Land, das besonders stark durch Banking Trojaner bedroht wird. Hier bedienten sich die Cyberkriminellen besonders häufig der Trojaner Dyreza, Dridex und Zbot ebenso wie Qbot, der in den USA im weltweiten Vergleich im Übrigen ungewöhnlich häufig vorzufinden ist. Cryptoware ist die verbreitetste Ransomware, auch zu finden ist aber CTBLocker. Zudem konnten die SophosLabs Experten eine hohe Zahl von bunitu (Proxyschadware) und der Dateien-Infektions-Software MPhage ausmachen.

Kanada hat es am häufigsten mit Ransomware zu tun – hier waren Cryptowall, CTBLocker und teslacrypt am verbreitetsten – gefolgt von Angriffen durch Banking Trojaner, namentlich Dyreza, Zbot, Vawtrak, Dridex und – eher ungewöhnlich – Tinba.

Südamerika
Brasilien wird vor allem mit Ransomware und Spam überschüttet mit Cryptowall und Fareit als Top-Vertreter der jeweiligen Kategorie.
Interessantes zeigte sich auf diesem Kontinent in Kolumbien: hier fanden die Sophos Labs Forscher eine große Anzahl des Remote Access Trojaners xtrat, der, wie der Name sagt, von außen direkten Zugriff auf ein System erlaubt.

Afrika

Südafrika ächzt besonders unter Spamfluten, verteilt durch Shapouf. Auch die anderen Kategorien der Malware sind vertreten, hier durch die Banking Trojaner Dridex und Zbot, die Ransomware Cryptowall sowie den Downloader Upatre.

Mittlerer Osten

Wenig überraschend ist, dass auch Saudi Arabien mit Banking Trojanern – hier insbesondere Dyreza, Zbot und Dridex sowie Ransomware (Cryptowall) zu kämpfen hat. Aber auch Angriffe durch Malware für Passwort Diebstahl (Fareit) sowie extrem viele RAT-Angriffe, also “ferngesteuerten” unerlaubten Zugriff auf Systeme hatte das Land zu verkraften.

Bei Türkischen Cyberkriminellen sind vor allem Downloader wie upatre hoch im Kurs. Ransomware ist ebenfalls stark vertreten durch Cryptowall and TorrentLocker. Und auch in der Türkei bedient man sich mit Vorliebe eines Remote Access Trojaners (RAT), namentlich Bladabindi, der in einer ungewöhnlich hohen Zahl anzutreffen ist.

Asien

In Indien findet sich eine signifikant hohe Zahl von Würmern wie Jenxcus oder Dorkbot und Viren, hier ganz speziell Quervar. Ebenfalls in Vielzahl vertreten sind die Banking Malware Dridex, der Downloader Upatre und der Spambot Shapouf.

Chinas Malware-Szene setzt ganz klar und mit großem Abstand auf Spam. Außerdem ist im bevölkerungsreichsten Land der Erde schadhafte Downloadsoftware (Upatre, Ruckguv) stark vertreten.

Japan sieht sich einer großen Zahl von Angriffen durch Banking Trojaner ausgesetzt (Zbot, qbot, Dridex, yebot) und wird außerdem vermehrt durch Spambots (Shapouf) und Ransomware, hier speziell Cryptowall, bedroht.

Für Singapur verzeichneten die SophosLabs eine hohe Zahl von Würmern (Dorkbot, Jenxcus), aber auch Downloader Upatre, Passwort-Dieb Fareit und Ransomware Cryptowall in großer Anzahl.

Auch Malaysia zeigt, ähnlich wie Indien, ein hohes Aufkommen von Würmern (Dorkbot, Lethic) und neben den für Singapur bereits genannten Kategorien auch eine starke Verbreitung des Spambots Shapouf.

In Honkong überrascht die Tatsache wenig, dass es sich bei der Metropole um eine Hochburg für Banking Trojaner (Dridex, yebot, Zbot, emotet, Dyreza) handelt. Auch stark vertreten sind Password Stealers (Fareit).

Auf den Philippinen treiben Würmer wie Dorkbot und Lethic ihr extremes Unwesen, nicht viel weniger häufig sind auch Spambots.

Australien

Eine Besonderheit fanden die Sophos Labs Experten in Australien. Hier verzeichneten sie eine ungewöhnliche hohe Zahl des Bootkit Cidox und der Ransomware VirRnsm (Viral Ransomware). Ebenfalls hoch war die Zahl von Ransomware und Banking Trojanern wie Tinba.

Glossar der genannten Bedrohungen

Threat	Aliases	Category
upatre		Downloader
Cryptowall	Cryptowall	Ransomware
fareit	Pony	Password stealer
dridex	Bugat,Geodo	Banking
shapouf		Spambot
emotet	Feodo	Banking
zbot	Zeus,Citadel,KINS,IceIX	Banking
ruckguv		Downloader
dorkbot		Worm
dyreza	Dyre,Dyzap	Banking
necurs		Rookit,Downloader
tinba	Tiny Banker,Zusy	Banking
qbot	Qakbot	Worm,Banking
jenxcus	NJ Worm	Worm,RAT
TorrentLocker	TorrentLocker	Ransomware
gozi	Ursnif,Papras	Banking
CTBLocker	CTBLocker	Ransomware
Ramnit		Banking,worm,File infector
Chir		File infector
Sality		File infector
Bondat		JS Downloader
xtrat	Xtreme RAT	RAT
limitless	Hawkeye,Predator Pain	Keylogger, password stealer
trustezeb	Matsnu	Banking
lethic		Worm
bladabindi	NJ RAT	RAT
newposthings	Bagopos, Punkey	POS
cidox	Rovnix	Bootkit, Downloader
yebot	Tilon	Banking
MPhage	PDFCrypt	File infector
Expiro		File infector
Parite		File infector
VirRnsm	Viral Ransomware	Ransomware
Bursted		Autocad file infector

Conficker		Worm
Quervar		File infector
xswkit	Gootkit	Downloader,Click fraud
bunitu		Proxy

Über Sophos
Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.
Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de