DIE DARKHOTEL APT

EINE GESCHICHTE UNGEWÖHNLICHER GASTFREUNDSCHAFT

Version 1.1
November 2014

Global Research and Analysis Team

KASPERSKY lab

Inhaltsverzeichnis

Zusammenfassung

Darkhotel APT ist ein Bedrohungsakteur mit Eigenschaften, die auf den ersten Blick uneinheitlich und sogar widersprüchlich sind, wobei einige der Fähigkeiten sehr weit entwickelt, andere dagegen eher rudimentär zu sein scheinen. Diese Bedrohung besteht seit fast einem Jahrzehnt, und nun schlägt der „ungebetene Gast“ wieder zu. Die offensiven Aktivitäten des Akteurs finden meist über die Wi--Fi- und physischen Verbindungen bestimmter Hotels und Geschäftszentren statt, wobei aber auch Peer-to-Peer- (p2p) und File-Sharing-Netzwerke sowie durch Spearfishing ausgewählte Opfer angegriffen wurden. Als Darkhotel-Tools wurden u. a. „Tapaoux”, „Pioneer”, „Karba” und „Nemim” nachgewiesen. Die folgende Aufstellung liefert einen Überblick über die wichtigsten Eigenschaften der Angreifergruppe:

- operative Kompetenz, globale und vertrauenswürdige Netzwerkressourcen über Jahre hinaus mit strategischer Präzision zu kompromittieren, zu missbrauchen und einen ständigen Zugriff darauf zu gewährleisten
- hoch entwickelte mathematische und kryptoanalytische Offensivfähigkeiten gepaart mit der skrupellosen Ausnutzung des Vertrauens in Zertifizierungsstellen und die Public-Key-Infrastruktur
- willkürliche Infektion von Systemen mit eingeschränkter regionaler Unterscheidungsfähigkeit zwischen vertrauenswürdigen und nicht vertrauenswürdigen Ressourcen für den Aufbau und Betrieb von groß angelegten Botnets
- gut entwickelte Keylogger auf niedriger Ebene innerhalb eines effektiven und einheitlichen Toolsets
- Konzentration auf bestimmte Kategorien von Angriffszielen innerhalb von Kampagnen und deren Markierung

- eine umfangreiche, dynamische Infrastruktur aus Apache-Webservern, dynamischen DNS-Datensätzen, Kryptobibliotheken und PHP-Webapps
- regelmäßige Zero-Day-Nutzung – kürzliche Bereitstellung eines integrierten Adobe Flash Zero-Day-Spearphishing-Exploits und gelegentliche Bereitstellung anderer Zero-Day-Ressourcen für umfangreiche, mehrere Jahre andauernde Kampagnen

Einleitung

Nichts ahnende Gäste, darunter leitende Angestellte und Unternehmer aus dem Technologiesegment, die sich möglichen Angriffen bewusst sind, werden bei der Nutzung des Internets in einer Vielzahl unterschiedlicher Hotels mit einem seltenen APT-Trojaner infiziert, der sich als ein wichtiges Software-Update ausgibt. Dabei kann es sich z. B. um Updates für GoogleToolbar, Adobe Flash, Windows Messenger etc. handeln. Diese erste Infektionsphase ermöglicht es den Angreifern, vielversprechende Angriffsziele ausfindig zu machen und hoch entwickelte Diebstahl-Tools auf das Zielsystem herunterzuladen.

Die Installationen werden gezielt über das Hotelnetzwerk auf die Geräte der angegriffenen Personen verteilt. Es ist davon auszugehen, dass die Gruppe schon im Voraus darüber Bescheid weiß, wann die Zielpersonen in ihren Luxusunterkünften eintreffen und diese wieder verlassen. Die Angreifer liegen also so lange auf der Lauer, bis ein Opfer in seinem Hotel eincheckt und eine Verbindung zum Internet herstellt.

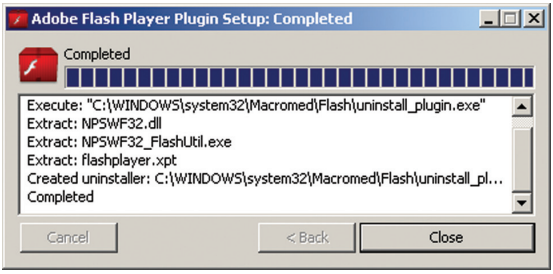
Das FBI hat Sicherheitshinweise zu ähnlich gelagerten Vorfällen in Hotels herausgegeben, und auch australische Regierungsbeamte waren von ähnlichen Malware-Infektionen betroffen. Eine der Verlautbarungen des FBI zu Cyberangriffen auf Hotelgäste im Ausland stammt von Mai 2012, aber entsprechende Darkhotel-Proben waren bereits im Jahr 2007 im Umlauf. Verfügbare Verbindungsprotokolle von Darkhotel-Servern gehen auf den 1. Januar 2009 zurück. Außerdem beweist die Infizierung von p2p-Netzwerken mit weit verbreiteter Malware und Zero-Day-Phishing-Attacken, dass hinter der fragwürdigen Gastfreundlichkeit, die Darkhotel APT seinen Gästen gegenüber an den Tag legt, ein effektives Toolset und ein langfristig angelegter Einsatz stecken.

Analyse

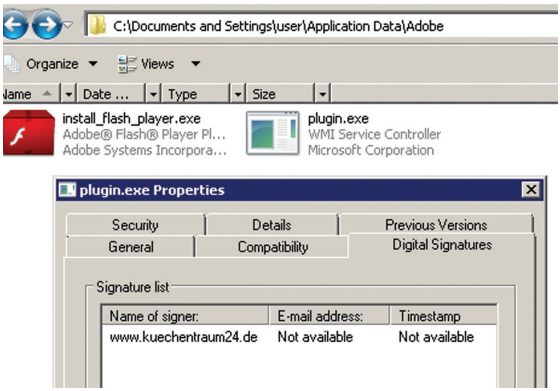
Einschleusung – Hotels/Geschäftszentren und willkürliche Verbreitung

Verbreitung über Hotels und Geschäftszentren

Die gezielte Verbreitung der Darkhotel APT-Malware konnte in einer Reihe von Hotel-Netzwerken beobachtet werden: Besucher, die sich beim Wi-Fi-Netzwerk eines Hotels anmeldeten, wurden aufgefordert, Updates für gängige Softwarepakete zu installieren.



Natürlich handelte es sich dabei in Wirklichkeit um Installationsroutinen für die Darkhotel-Backdoorprogramme, die den echten Installationsprogrammen von Adobe und Google hinzugefügt wurden. Digital signierte Darkhotel-Backdoors wurden so zusammen mit den legitimen Softwarepaketen installiert.



Der wohl interessanteste Aspekt an dieser Verbreitungsmethode ist, dass zur Anmeldung im Hotel-Netzwerk der Nachname und die Zimmernummer des Gasts erforderlich sind, aber nur einige wenige Gäste mit dem Darkhotel-Paket infiziert wurden. Beim Besuch derselben Hotels schaffte es unser „Lockvogel"-System nicht, die Aufmerksamkeit der Darkhotel-Angreifer auf sich zu ziehen. Diese Daten sind wenig aussagekräftig, deuten aber auf den Missbrauch von Hotel-Anmeldeinformationen hin.

Missbrauch der Netzwerkinfrastruktur

Der Darkhotel-Akteur behielt in den Hotelnetzwerken ein effektives „Intrusion Set" bei, das ihm über Jahre hinaus hinreichend Zugang zu unerwarteten Angriffspunkten bot. Diese Bereitstellungspunkte boten den Angreifern darüber hinaus Informationen über Anreise und Abreise sowie Angaben zur Identität der Gäste von Luxushotels.

Als Teil einer noch laufenden Untersuchung führte unsere Analyse uns zu eingebetteten iframes innerhalb von Hotelnetzwerken, über die die Webbrowser der Gäste zu den gefälschten Installationsprogrammen umgeleitet wurden. Die Angreifer gingen bei der Platzierung der iframes und ausführbaren Dateien innerhalb von vertrauten Ressourcen – also den Anmeldeportalen der Hotels – sehr vorsichtig vor. Darüber hinaus wurden auch alle Spuren, die von ihren Tools hinterlassen wurden, nach dem erfolgreichen Abschluss einer Attacke umgehend beseitigt. Derzeit werden die betroffenen Portale analysiert, bereinigt und einer weiterführenden Untersuchung und Sicherheitshärtung unterzogen. Ende 2013 und Anfang 2014 konnten wir Spuren eines solchen Vorfalls in einem Hotelnetzwerk beobachten. Die Angreifer richteten ihre Umgebung ein und trafen präzise das anvisierte Ziel. Sobald das Angriffsziel wieder abgereist war und das Angriffs-Frame geschlossen wurde, wurden das platzierte iframe und die Backdoorprogramme aus dem Hotelnetzwerk entfernt. In einem anderen Hotel beseitigten die Angreifer die Spuren eines vorherigen Angriffs, ihre Angriffsmethoden waren jedoch dieselben. Externe Meldungen zu ähnlichen Vorgängen in anderen Hotels bestätigen auch dort dieselbe, äußerst vorsichtige Vorgehensweise.

Hierbei kommt es zu einer Vermischung von gängigen APT-Taktiken, ziemlich nachlässig aufgebauten „Watering-Hole-Attacken" bzw. einer „strategischen Kompromittierung von Websites" und präziseren Spearphishing-Methoden. In diesem Fall wartet das Darkhotel-Team darauf, dass sich das Opfer per Hotel-Wi-Fi oder Kabel mit dem Internet verbindet. Es ist sehr wahrscheinlich, dass die Angriffsziele eine Verbindung über diese Ressourcen herstellen, und die Angreifer machen sich diesen Umstand zunutze. Die Angreifer verfügen zudem über ge-

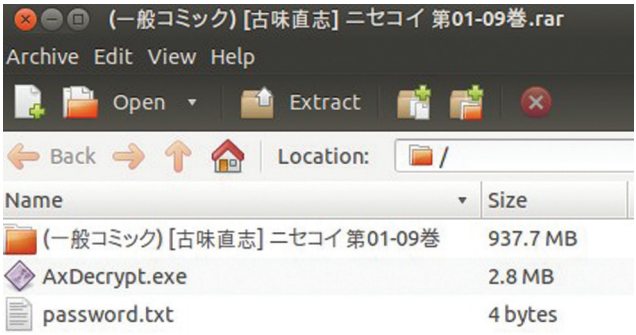
naue Informationen zum Aufenthalt ihrer Opfer, ähnlich wie sie bei einer Spearfishing-Attacke über die E-Mail-Adresse und die inhaltlichen Interessen ihrer Opfer informiert wären. Bei der Vorbereitung des Angriffs waren den Darkhotel-Angreifern u. a. die voraussichtliche Ankunfts- und Abreisezeit, die Zimmernummer und der vollständige Name des Opfers bekannt. Auf diese Weise waren sie in der Lage, den infizierten iframe gezielt dem gewünschten Angriffsziel zu präsentieren. Hier zeigt sich also eine weitere einzigartige Charakteristik dieser Angreifergruppe – sie bedient sich einer ausreichend treffsicheren, aber gleichzeitig hochpräzisen Angriffsmethode.

Willkürliche Verbreitung

Ein Beispiel für die willkürliche Verbreitung von Malware durch Darkhotel APT ist die Art und Weise, wie japanische p2p-Sharing-Sites infiziert werden. Die Verbreitung der Malware erfolgt hier über ein umfangreiches (ca. 900 MB großes) rar-Archiv. Wie unten beschrieben wird das Archiv auch über Bittorrent zum Download angeboten. Darkhotel nutzt diese Methode zur Verbreitung seines Karba-Trojaners. Diese japanischen Archive, die für chinesischsprachige Benutzer übersetzt wurden, haben offensichtlich sexuellen Charakter und sind Teil einer Reihe von Sex-/Militär-Anime-Comics, mit denen die möglichen Interessen von potentiellen Angriffszielen bloßgestellt werden sollen.

Dieses Darkhotel-Paket wurde in weniger als sechs Monaten mehr als 30.000 Mal heruntergeladen. Das hier aufgeführte p2p-Angebot von Darkhotel wurde am 22.11.2013 gepostet. Die Verbreitung fand im gesamten Jahr 2014 statt.

（一般コミック）［古味直志］ニセコイ 第01–09巻.rar



Über das betreffende Torrent wird eine fast 900 MB große Datei heruntergeladen. Das rar-Archiv wird in ein Verzeichnis mit einer Vielzahl verschlüsselter Zips mit-

samt zugehörigem Decodierer und einer Kennwortdatei zur Entschlüsselung der Zips dekomprimiert. Tatsächlich ist jedoch der angebliche Decodierer „AxDecrypt.exe“ sowohl mit dem eigentlichen Decodierer und dem Dropper für den Darkhotel-Karba-Trojaner „Catch.exe“ gekoppelt. Lädt ein Benutzer den Torrent herunter und entschlüsselt die enthaltenen Zip-Dateien, wird dabei der Trojaner heimlich installiert und auf dem Zielsystem ausgeführt.

Catch.exe, nachgewiesen als Backdoor.Win32.Agent.dgrn, kommuniziert mit folgenden Command-and-Control-Servern von Darkhotel:

microdelta.crabdance.com microyours.ignorelist.com micronames.jumpingcrab.com microchisk.mooo.com microalba.serveftp.com

Dieses in geteilte Torrents eingebundene Darkhotel-Backdoorprogramm findet sich beispielsweise auch noch in japanischen Anime-Comics mit nicht-jugendfreien Inhalten. Die betreffenden Torrents wurden mehrere zehntausend Mal heruntergeladen.

„torrent\[hgd资源组][漫画]comic1☆7漫画合集③+④+⑤+特典[5.08g][绅士向][总第四十三弹]（七夕节快乐！）\汉化\(comic1☆7）[莉零（小鹿りな，古代兵器)] 凌 -shinogi-（闪乱カグラ）[中文] “

und

„動漫\[hgd资源组][漫画]comic1☆7漫画合集③+④+⑤+特典[5.08g][绅士向][总第四十三弹]（七夕节快乐！）\汉化”）

Das zugehörige Darkhotel-Backdoorprogramm wurde auf Bittorrent, emule etc. unter einer Vielzahl unterschiedlicher Bezeichnungen für Comics gehostet. Hierzu gehören z. B. Angebote für Comics und Anime-Inhalte. Hier einige Beispiele für die zugehörigen Command-and-Control-Server von Darkhotel:

microblo5.mooo.com microyours.ignorelist.com micronames.jumpingcrab.com microchisk.mooo.com microalba.serveftp.com

Spearphishing-Kampagnen von Darkhotel

Darkhotel-Kampagnen, bei denen in der Regel per Spearphishing eingeschleuste Tapaoux-Implantate eingesetzt werden, sind in den letzten fünf Jahren immer wieder vereinzelt aufgetreten. Diese Teilprojekte hatten es auf den Rüstungssektor, Behörden und NGOs abgesehen. E-Mail-Inhalte zu Themen wie Nuklearenergie und militärische Fähigkeiten wurden dabei als Köder eingesetzt. Erste Berichte mit Beschreibungen von Angriffen auf nichtstaatliche Organisationen und staatliche Entscheidungsträger wurden auf contagio veröffentlicht. Diese Spearfishing-Aktivität wurde auch 2014 fortgesetzt. Die Angriffe folgen dem typischen Spearphishing-Muster, und in den letzten Monaten haben die infiltrierten Systeme Downloader-Programme von Webservern wie hxxp://office-revision.com/update/files22/update.exe oder hxxp://trade-inf.com/mt/ duspr.exe abgerufen.

In den letzten Jahren hat die Gruppe E-Mail-Links verschickt, welche die Browser der angegriffenen Benutzer zu einem Zero-Day-Exploit für Internet Explorer umleiten. Manchmal enthält auch der Anhang selbst ein Zero-Day-Exploit für Adobe.

Aktueller Einsatz von Zero-Day-Exploits

Diese Angreifergruppe arbeitet gelegentlich auch mit Zero-Day-Exploits, vernichtet diese aber wieder, falls erforderlich. In den letzten Jahren setzte sie gezielte Zero-Day-Spearphishing-Attacken ein, die Adobe-Produkte und Microsoft Internet Explorer zum Ziel hatten, darunter auch cve-2010-0188. Anfang 2014 deckten unsere Analysten die Verwendung von cve-2014-0497 auf, einem Zero-Day-Exploit für Flash, das Anfang Februar auf Securelist beschrieben wurde.

Die Gruppe startete eine Spearfishing-Attacke auf Systeme mit chinesischen ISPs und stattete die Zero-Day-Exploits mit Fähigkeiten aus, die es ihnen erlaubten, auch mit gehärteten Windows 8.1-Systemen fertig zu werden. Interessanterweise waren die Flash-Objekte in koreanische Dokumente mit dem folgenden Titel eingebettet „List of the latest Japanese AV wind and how to use torrents.docx" (ungefähre Übersetzung ins Englische). Das abgesetzte Downloader-Programm (d8137ded710d83e2339a97ee78494c34) lud dann Schadcode ähnlich der weiter unten skizzierten und in Anhang D ausführlich beschriebenen „Information Stealer"-Komponente herunter.

Digitale Zertifikate und Entlegitimierung von Zertifizierungsstellen

Darkhotel signiert seine Backdoorprogramme in der Regel mit einer Reihe unterschiedlicher digitaler Zertifikate. Die ursprünglich von dieser Gruppe gewähl-

ten Zertifikate sind jedoch aufgrund ihrer schwachen Schlüssel und der hohen Missbrauchswahrscheinlichkeit sehr interessant. Die folgende Übersicht enthält die Zertifikate, die normalerweise zur Signierung von Darkhotel-Schadcode eingesetzt wurden. Sie erfordern hoch entwickelte mathematische Fähigkeiten, um die Schlüssel zum jeweiligen Zeitpunkt zu faktorisieren. Sie sind nicht die einzigen von der Gruppe eingesetzten Zertifikate. Jüngste Aktivitäten lassen darauf schließen, dass die Gruppe gestohlene Zertifikate zum Signieren ihrer Schadcodes einsetzt.

Stammzertifizierungsstelle	Untergeordnete Zertifizierungs-/Ausgabestelle	Inhaber	Status	Gültig ab	Gültig bis
GTE CyberTrust	Digisign Server ID (Enrich)	flexicorp.jaring.my sha1/RSA (512 Bit)	Abgelaufen	17.12.2008	17.12.2010
GTE CyberTrust	Cybertrust SureServer CA	inpack.syniverse.my sha1/RSA (512 Bit)	Widerrufen	13.12.2009	13.02.2011
GTE CyberTrust	Cybertrust SureServer CA	inpack.syniverse.com sha1/RSA (512 Bit)	Widerrufen	13.12.2009	13.02.2011
GTE CyberTrust	Anthem Inc Certificate Auth	ahi.anthem.com sha1/RSA (512 Bit)	Ungültige Signatur	13.01.2010	13.01.2011
GlobalSign	Deutsche Telekom CA 5	www.kuechentraum24.de sha1/RSA (512 Bit)	Widerrufen	20.10.2008	25.10.2009
GTE CyberTrust	Digisign Server ID (Enrich)	payments.bnm.gov.my sha1/RSA (512 Bit)	Ungültige Signatur	12.07.2009	12.07.2010
GTE CyberTrust	TaiCA Secure CA	esupplychain.com.tw sha1/RSA (512 Bit)	Abgelaufen	07.02.2010	17.07.2011
GTE CyberTrust	Digisign Server ID (Enrich)	mcrs2.digicert.com.my sha1/RSA (512 Bit)	Ungültige Signatur	28.03.2010	28.03.2012
GTE CyberTrust	Cybertrust SureServer CA	agreement.syniverse.com sha1/RSA (512 Bit)	Ungültige Signatur	13.12.2009	13.02.2011
GTE CyberTrust	Cybertrust SureServer CA	ambermms.syniverse.sha1/RSA (512 Bit)	Ungültige Signatur	16.02.2009	16.02.2011
Equifax Secure eBusiness CA-1	Equifax Secure eBusiness CA-1	secure.hotelreykjavik.is md5/RSA (512 Bit)	Ungültige Signatur	27.02.2005	30.03.2007

Stammzertifizierungsstelle	Untergeordnete Zertifizierungs-/Ausgabestelle	Inhaber	Status	Gültig ab	Gültig bis
GTE CyberTrust	Cybertrust Educational CA	stfmail.ccn.ac.uk sha1/RSA (512 Bit)	Ungültige Signatur	11.12.2008	11.12.2011
GTE CyberTrust	Digisign Server ID (Enrich)	webmail.jaring.my sha1/RSA (512 Bit)	Ungültige Signatur	06.01.2009	06.01.2011
GTE CyberTrust	Cybertrust Educational CA	skillsforge.londonmet.ac.uk sha1/RSA (512 Bit)	Ungültige Signatur	16.01.2009	16.01.2012
GTE CyberTrust	Digisign Server ID (Enrich)	anjungnet.mardi.gov. my sha1/RSA (512 Bit)	Ungültige Signatur	29.09.2009	29.09.2011
GTE CyberTrust	Anthem Inc Certificate Authority	dl-ait-middleware@anthem.com sha1/RSA (512 Bit)	Ungültige Signatur	22.04.2009	22.04.2010
GTE CyberTrust	Cybertrust Educational CA	ad-idmapp.cityofbristol.ac.uk sha1/RSA (512 Bit)	Ungültige Signatur	11.09.2008	11.09.2011
Verisign	Verisign Class 3 Secure OFX CA G3	secure2.eecu.com sha1/RSA (512 Bit)	Ungültige Signatur	25.10.2009	26.10.2010
Root Agency	Root Agency	Microsoft md5/RSA (1024 Bit)	Ungültige Signatur	06.09.2009	31.12.2039
GTE Cybertrust	CyberTrust SureServer CA	trainingforms.syniverse.com sha1/RSA (512 Bit)	Ungültige Signatur	17.02.2009	17.02.2011

Alle zugehörigen Fälle von signierter Darkhotel-Malware haben eine gemeinsame Stammzertifizierungsstelle und zwischengeschaltete Zertifizierungsstelle, die Zertifikate mit schwachen md5-Schlüsseln (RSA 512 Bit) ausgegeben haben. Wir sind uns sicher, dass der Darkhotel-Bedrohungsakteur diese Zertifikate vervielfältigt hat, um seine Malware damit zu signieren. Diese Schlüssel wurden nicht gestohlen. Viele dieser Zertifikate wurden in einem Fox-IT-Post aus dem Jahr 2011, „RSA-512 Certificates Abused in the Wild" erwähnt.

Die folgende unspezifische Sicherheitsempfehlung von Microsoft, die Mozilla-Empfehlung, mit der seinerzeit auf das Problem reagiert wurde, und die Reaktionen von Entrust stützen diese Vermutung.

Aus der Microsoft-Sicherheitsempfehlung vom 10. November 2011:

„Microsoft ist bekannt, dass DigiCert Sdn. Bhd, eine untergeordnete malaysische Zertifizierungsstelle (CA) unter Entrust und GTE CyberTrust, 22 Zertifikate mit schwachen 512-Bit-Schlüsseln veröffentlicht hat. Wenn diese schwachen Verschlüsselungsschlüssel entschlüsselt werden, kann ein Angreifer die Zertifikate in betrügerischer Absicht verwenden, um Inhalte nachzuahmen und Phishingangriffe oder Man-in-the-Middle-Angriffe gegen alle Webbrowser-Benutzer durchzuführen, einschließlich Benutzern von Internet Explorer. Dies ist zwar keine Sicherheitsanfälligkeit in einem Microsoft-Produkt, doch dieses Problem betrifft alle unterstützten Veröffentlichungen von Microsoft Windows.

Es gibt keine Hinweise, dass Zertifikate in betrügerischer Absicht ausgestellt wurden. Stattdessen konnten aufgrund kryptografisch schwacher Schlüssel einige der Zertifikate dupliziert und in betrügerischer Absicht verwendet werden.

Microsoft stellt ein Update für alle unterstützten Veröffentlichungen von Microsoft Windows bereit, mit denen das Vertrauen in DigiCert Sdn. Bhd. widerrufen wird. In diesem Update wird das Vertrauen gegenüber den beiden folgenden vorläufigen CA Zertifikaten widerrufen: Digisign Server ID – (Enrich), veröffentlicht von der Zertifizierungsstelle Entrust.net (2048) und **Digisign Server ID (Enrich)**, veröffentlicht von **GTE CyberTrust Global Root**"

Aus der Reaktion von Mozilla (2011):

„Obwohl es k**einen Hinweis darauf gibt, dass die Zertifikate in betrügerischer Absicht ausgestellt wurden, haben es die schwachen Schlüssel ermöglicht, sie zu kompromittieren.** Außerdem weisen die Zertifikate von dieser Zertifizierungsstelle eine Reihe von technischen Fehlern auf. Ihnen fehlt eine EKU-Erweiterung zur Angabe der beabsichtigten Verwendung, und sie wurden ohne Informationen zum Widerruf ausgestellt."

Aus der Reaktion von Entrust:

„Es gibt keinen Beweis dafür, dass die Digicert Malaysia-Zertifikate kompromittiert wurden."

Die Schlüssel knacken

Es folgen einige Anmerkungen zu den Kosten und technischen Voraussetzungen, die erforderlich sind, um die Schlüssel für diese Zertifikate zu knacken.

Die Rechenleistung, die zum Knacken und Faktorisieren eines RSA 512-Bit-Schlüssels erforderlich war, kostete 5000 US-Dollar. Der Vorgang dauerte ca.

zwei Wochen. (siehe http://lukenotricks.blogspot.co.at/2010/03/rsa-512-factoring-service-two-weeks.html)

Im Oktober 2012 berichtete Tom Ritter, dass dies 120 - 150 US-Dollar, möglicherweise sogar nur ganze 75 US-Dollar koste.

Das von D.J. Bernstein 2001 vorgelegte Dossier zur Konstruktion eines Computers, mit dem die Kosten der Ganzzahlenfaktorisierung mithilfe von Zahlkörpersiebverfahren reduziert werden, die in der Lage sind, RSA-Schlüssel mit 1024 Bit zu knacken.

Die Stellungnahme von RSA (2002) dazu, ob 1024-Bit-RSA-Schlüssel geknackt wurden: „NIST hat bei seinem Workshop zum Schlüssel-Management im November 2001 unterschiedliche Schlüsselgrößen zur Diskussion gestellt [7]. Für Daten, die ab 2015 keinen Schutz mehr benötigen, wird eine RSA-Schlüsselgröße von mindestens 1024 Bit vorgeschlagen. Für Daten, die auch noch darüber hinaus verschlüsselt werden müssen, sind mindestens 2048 Bit erforderlich."

Weitere Tapaoux-Zertifikate

Die jüngsten Tapaoux-Angriffe und Backdoorprogramme beinhalten Malware, die mit starken, durch 2048-Bit-Schlüssel geschützten SHA1/RSA-Zertifikaten signiert wurden, was Zertifikatsdiebstahl nahelegt.

Stammzertifizierungsstelle	Untergeordnete Zertifizierungs-/Ausgabestelle	Inhaber	Status	Gültig ab	Gültig bis
thawte	thawte Primary Root CA	Xuchang Hongguang Technology Co.,Ltd. sha1/RSA (2048 Bit)	Widerrufen	18.07.2013	16.07.2014
thawte	thawte Primary Root CA	Ningbo Gaoxinqu zhidian Electric Power Technology Co., Ltd. sha1/RSA (2048 Bit)	Widerrufen	11.05.2013	11.05.2014

Hochentwickelte Keylogger

Einer der interessantesten Aspekte dieser Kampagne war die Verwendung eines digital signierten, hoch entwickelten Keylogger. Es handelt sich dabei um sauberen, gut geschriebenen Schadcode auf Kernel-Ebene. Die Strings sind auf Englisch und Koreanisch verfasst. Signiert wird er mit dem gängigen digitalen Zertifikat von „belinda.jablonski@syniverse.com".

Der Keylogger wird von Code abgelegt, der innerhalb von svchost.exe unter WinXP SP3 ausgeführt wird und einen interessanten Debug-String enthält: d:\KerKey\KerKey(일반)\KerKey\release\KerKey.pdb

Anmerkung: 일반 bedeutet im Koreanischen „Generalschlüssel".

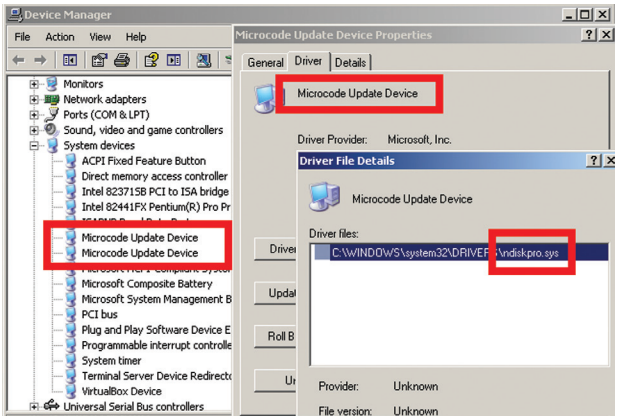
Der Keylogger wurde wahrscheinlich im Rahmen eines Projekts aus dem Jahr 2009 entwickelt:
e:\project\2009\x\total_source\32bit\ndiskpro\src\ioman.c

Keylogger-Code

Dieses Treiberpaket wurde so konstruiert, dass es einem echten Microsoft-Low-Level-Systemgerät ähnelt. Es wird als Systemkernel-Treiberdienst namens „Ndiskpro" mit der Beschreibung „Microcode Update Device" installiert. Es ist verwunderlich, dass der Dienst nicht durch eine Rootkit-Funktion verborgen wird:

```
SERVICE_NAME: Ndiskpro
DISPLAY_NAME: Ndiskpro
        TYPE               : 1  KERNEL_DRIVER
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms
```

Nach dem Laden hakt sich der Treiber NDISKPRO.SYS sowohl bei INT 0x01 und INT 0xff ein und ruft die Tastaturanschlagsdaten direkt über Port 0x60 ab, dem eigentlichen Motherboard-Tastaturcontroller. Die protokollierten Benutzerdaten werden gepuffert und dann an die aktive Benutzermoduskomponente übermittelt. Diese Komponente entschlüsselt dann die abgerufenen Werte und schreibt sie in eine zufällig benannte temporäre Datei, z. B. ffffz07131101.tmp. Diese Datei wird in demselben Verzeichnis erstellt, in dem sich das Dropper-Programm befindet, welches durch eine simple Erweiterung des „Run"-Eintrags in der Registrierungsdatenbank persistent bleibt.



Wie bereits erwähnt, verschlüsselt und speichert das Keylogger-Modul die erfassten Daten in einer Protokolldatei. Der verwendete Verschlüsselungsalgorithmus ähnelt RC4. Interessanterweise wird der Schlüssel zufällig durch das Modul generiert und an einem sehr ungewöhnlichen Ort abgelegt: innerhalb des Protokolldateinamens. Der numerische Teil des Dateinamens wird folglich als Ausgangspunkt für den Pseudozufallszahlengenerator verwendet. Die Zufallsfunktion wird statisch verknüpft, um dieselben Ergebnisse auf verschiedenen Computern zu gewährleisten.

Interessante Malware-Komponenten

Das Darkhotel-Toolset besteht aus einer Vielzahl von Komponenten, die im Lauf der Zeit geringfügig modifiziert wurden. Die Tools werden von Installationsroutinen in Hotelnetzwerken eingeschleust, die legitime Software-Installationsroutinen nachahmen. Sie sind in Torrent-Dateipakete eingebunden oder werden durch Exploits bzw. über Hyperlinks aus Spearphishing-E-Mails eingeschleust.

Hoch entwickelte Tools wie der oben beschriebene Keylogger werden zu einem späteren Zeitpunkt durch eines der folgenden Implantate auf das Zielsystem heruntergeladen. In einem aktuellen Fall legten Word-Dokumente, in denen swf-Dateien mit Zero-Day-Flash-Exploits eingebettet waren, die Backdoorprogramme entweder selbst ab oder luden diese von Remote-Webservern herunter und führten sie aus. Die Tools laden den Keylogger herunter, entwenden Informationen aus dem System oder laden andere Tools herunter.

- Small Downloader
- Information Stealer
- Trojaner
- Dropper und Self-Injector
- Selective Infector

Zu den interessantesten Verhaltensweisen dieser Komponenten gehören u. a:

- höchst ungewöhnliche, situationsabhängige 180-tägige Verzögerung der Kommunikation mit dem C&C-Server
- Selbstvernichtungsroutine, wenn die Standardcodepage des Systems auf Koreanisch umgestellt wird
- hoch entwickelte Vorgehensweise beim Diebstahl von Microsoft IntelliForm-Authentifizierungsinformationen
- Infostealer-Modul unterstützt Internet Explorer, Firefox und Chrome
- Aufrechterhaltung der ID während Kampagne oder Phase
- Empfindlichkeit für VM-Ausführung
- selektive virale Infektionsroutinen zur gezielten Ausführung der Malwareverbreitung innerhalb von Organisationen
- signierter Schadcode (siehe oben)

Small Downloader

Dieses Modul ist vergleichsweise klein (27 KB) und Teil der WinRar-SFX-Datei, welche die Datei ablegt und das Modul unter %APPDATA%\Microsoft\Crypto\DES64v7\msieckc.exe ausführt. Das Modul dient dazu, Schadkomponenten durch wiederholten Abgleich mit dem C&C-Server zu aktualisieren. Darüber hinaus kann es auch einige der veralteten Komponenten entfernen, deren Namen fest im Hauptteil des Schadcodes codiert sind. Das Modul fügt autorun-Registrierungseinträge hinzu, um einen automatischen Start während des Systemstarts zu ermöglichen.

Eine der interessantesten Funktionen dieses Moduls ist seine ungewöhnliche Ausführungsverzögerung und Persistenz. Wenn eine spezielle Datei im System vorhanden ist, nimmt das Modul erst dann Verbindung zu seinem C&C-Server auf, wenn die Datei 180 Tage alt ist. Wurde eine andere wichtige Schadkomponente innerhalb dieses Zeitraums entfernt, wird der Zugang zum System durch das aktuelle Modul innerhalb von sechs Monaten wiederhergestellt.

Die Komponente sammelt Systeminformationen und sendet diese an die Darkhotel-C&C-Server (siehe Beschreibung in Anhang D).

Information Stealer

Dieses Modul ist relativ groß (456 KB) und Teil der WinRar-SFX-Datei, welche die Datei ablegt und das Modul unter %APPDATA%\Microsoft\Display\DmaUp3.exe. startet. Das Modul dient hauptsächlich dazu, verschiedene vertrauliche Informationen auf lokalen Systemen zu erfassen und diese dann an die C&C-Server von Darkhotel zu übermitteln:

- Von Internet Explorer 6/7/8/9 zwischengespeicherte Kennwörter (Windows Protected Storage)
- In Mozilla Firefox (<12.0) gespeicherte vertrauliche Daten
- In Chrome gespeicherte vertrauliche Daten
- Zugangsdaten für Gmail Notifier
- Von Intelliform verwaltete Daten und Zugangsdaten:
  - Twitter
  - Facebook
  - Yandex
  - Qip
  - Nifty

- Mail.ru
- 126.com email
- Zapak
- Lavabit (verschlüsselter E-Mail-Service, der mittlerweile geschlossen wurde)
- Bigstring
- Gmx
- Sohu
- Zoho
- Sina
- Care2
- Mail.com
- Fastmail
- Inbox
- Gawab (E-Mail-Service aus dem Nahen Osten)
- 163.com
- Lycos
- Lycos mail
- Aol-Benutzernamen
- Yahoo!- Benutzernamen
- Yahoo!- Benutzernamen aus Japan
- Microsoft Live-Benutzernamen
- Google-Zugangsdaten

Dieses Modul ist so konzipiert, dass es sich auf Windows-Systemen selbsttätig vernichtet, wenn die Standardcodepage auf Koreanisch gesetzt wird.

Trojan.Win32.Karba.e

Diese Malware ist 220 KB groß. Sie wurde als MFC-Anwendung mit einer Vielzahl zusätzlicher Funktionsaufrufe konzipiert, die die Analyse der Probe normalerweise erschwert hätten. Sie ahmt eine grafische Desktopanwendung nach, generiert aber keine sichtbaren Fenster oder Dialogfelder für die Interaktion mit dem Benutzer. Der Trojaner sammelt Daten über das System und die darauf installierte Anti-Malware-Software und übermittelt die Informationen an die Darkhotel-C&C-Server. Weitere technische Details hierzu finden Sie in Anhang D.

Trojan-Dropper und Injector (infizierte legitime Dateien)

Diese Malware ist 63 KB groß. Sie ist mit einer Reihe anderer Softwarepakete gebündelt, die unterschiedliche Namen haben können, das Gesamtpaket wurde bisher aber durchgängig als „Virus.Win32.Pioneer.dx. Es setzt die „selective infector"-Komponente „igfxext.exe" auf dem Datenträger ab und führt sie aus.

Selective Infector

Bei dieser Komponente handelt es sich um einen **Virus**, der eingesetzt wird, um andere Computer selektiv per USB oder Netzwerkfreigaben zu infiltrieren.

Zuerst ruft der Virus alle verfügbaren Datenträger ab, sucht beginnend mit Datenträger 4 (D:\) bis hin zu Datenträger 20 (Z:\) nach allen ausführbaren Dateien und infiziert sie dann. Der Code arbeitet dabei mechanisch die Liste der verknüpften Wechseldatenträger ab.

Während des Infektionsvorgangs ändert der Infector den Einstiegspunkt der Programmdatei, generiert einen .rdat-Abschnitt, fügt dort eine kurze Laderoutine ein und setzt dann seine eigentliche Nutzlast in dem erstellten Overlay ab. Jede infizierte Datei besitzt Funktionen, die im Abschnitt zum Trojan-Dropper und Injector beschrieben werden. Auf diese Weise kann sie Informationen über den Computer sammeln, an den C&C-Server übermitteln und auf Befehl weitere Darkhotel-Komponenten herunterladen. Die nachgewiesenen heruntergeladenen Komponenten werden mit einem bekannten abgelaufenen Zertifikat von www.esupplychain.com.tw, signiert, das von Cybertrust SureServer CA ausgestellt wird.

Weitere technische Details hierzu finden Sie in Anhang D.

Kampagnen-Codes

Fast jedes Backdoorprogramm aus diesem Set führt einen internen Kampagnen-Code bzw. eine ID, die wie oben beschrieben bei der anfänglichen C&C-Kommunikation verwendet wird. Einige der IDs scheinen etwas mit geografischen Interessen zu tun zu haben, andere lassen sich nicht eindeutig zuordnen. Im Anschluss finden Sie eine Liste von Darkhotel-Kampagnen-IDs. Interne IDs und C&C-Ressourcen überschneiden sich bei diesen Komponenten, und auf Grundlage von Connectback-Ressourcen lässt sich kein eindeutiges Verteilungsmuster feststellen. Die am häufigsten vorkommende ID ist „DEXT87”:

DEXT87	NKstep2-auto
step2-auto	PANA(AMB)-auto
dome1-auto	PANA#MERA
step2-down	SOYA#2-auto
Java5.22	step2-down-u
C@RNUL-auto	(ULT)Q5SS@E.S-down
dome-down	VER1.5.1
M1Q84K3H	VICTORY
NKEX#V1.Q-auto	WINM#V1.Q

Infrastruktur und Angriffsziele

Dieses Infrastrukturteam scheint mit geringerer Kompetenz ausgestattet zu sein, als es bei hochrangigen Kampagnen der Fall ist. Es werden schwächere Serverkonfigurationen mit nur eingeschränkter Überwachung und Abwehrmaßnahmen eingesetzt, und es kommt zu einfachen Fehlern. Es gelingt jedoch, eine voll einsatzbereite Infrastruktur für neue und bestehende Infektionen aufrecht zu erhalten.

Insgesamt waren die Angriffsziele, die wir in unseren Sinkhole-Protokollen und KSN-Daten gefunden haben, über die gesamte Erde verteilt, wobei der Großteil aus Japan, Taiwan, China, Russland, Korea und Hong Kong stammte.

Sinkhole-Domänen

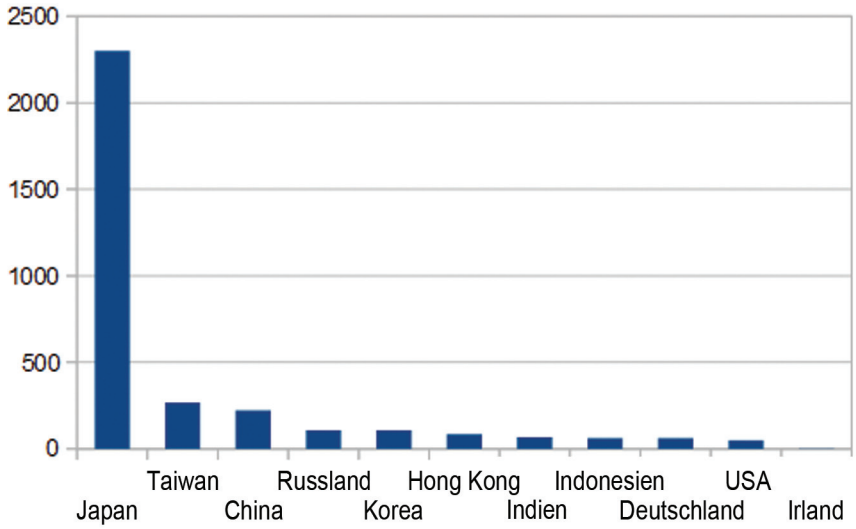
Die folgenden C&C-Domänen wurden per Sinkholing gebunden und an den Kaspersky Sinkhole Server umgeleitet:

42world.net
academyhouse.us
adobeplugs.net
amanity50.biz
autocashhh.hostmefree.org
autochecker.myftp.biz
autoshop.hostmefree.org
autoupdatfreeee.coolwwweb.com
checkingvirusscan.com
dailyissue.net
dailypatch-rnr2008.net
fenraw.northgeremy.info
generalemountina.com
goathoney.biz
jpnspts.biz
jpqueen.biz
mechanicalcomfort.net
micromacs.org
ncnbroadcasting.reportinside.net
neao.biz
private.neao.biz
reportinside.net
self-makeups.com
self-makingups.com
sourcecodecenter.org
support-forum.org
updatewifis.dyndns-wiki.com

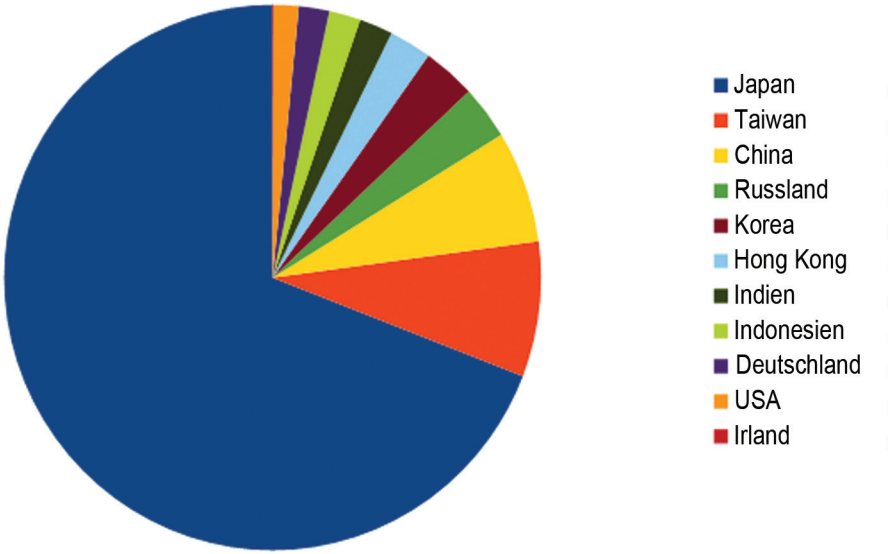
Verteilung von Angriffszielen gemäß KSN- und Sinkhole-Daten

KSN-Daten

Unser Kaspersky Security Network ermittelte Darkhotel-Infektionen auf Tausenden von Computern, meist in Zusammenhang mit den p2p-Kampagnen von Darkhotel. Diese Aufschlüsselung nach Geolokalisierungsdaten liefert wahrscheinlich das genaueste Bild über die geografische Verteilung der Darkhotel-Aktivitäten.

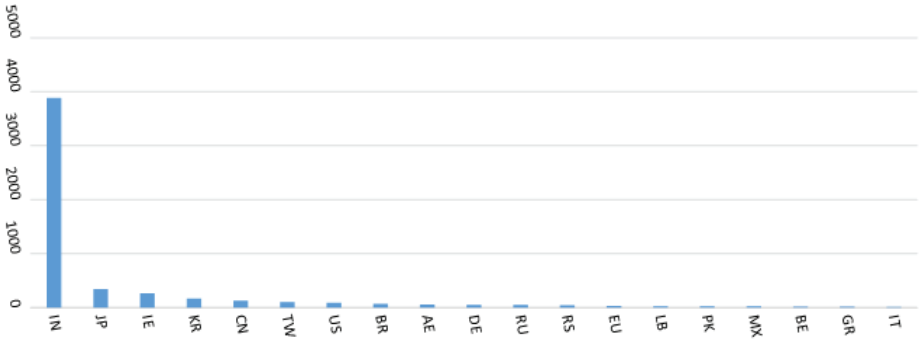


Das Tortendiagramm unten veranschaulicht die Verteilung der Darkhotel-Aktivitäten auf der ganzen Welt noch besser. Wie Sie sehen, verteilt sich über 90 % davon auf nur fünf Länder: Japan, gefolgt von Taiwan, China, Russland und Korea.



Sinkhole-Daten

Da die Betreiber bemüht sind, laufend neue C&C-Server in Betrieb zu nehmen, gestaltet sich das Sinkholing von genügend Domänen, um ein akkurates Bild der geografischen Verteilung der Angriffsziele zu ermöglichen, als schwierig. Hinzu kommt, dass auch viele Systeme, die nur Analysezwecken dienen, mit den per Sinkholing ermittelten Domänen verbunden sind. Das folgende Diagramm mit aktuellen Sinkhole-Rückrufen erlaubt jedoch schon erste Rückschlüsse über die geografische Verteilung der Angriffsziele, wobei Indien, Japan, Irland, Korea, China und Taiwan die vorderen Ränge belegen. Streicht man Indien und Irland aus diesem Set, steigt die Übereinstimmung mit unseren KSN-Daten.



Angriffszielstatistiken aus verfügbaren ddrlog-Dateien

Für viele dieser C2C-Server besteht ein Verzeichnispfad, über den ein ddrlog-Protokoll abgerufen werden kann. Im ddrlog werden offensichtlich Rückrufdaten geführt, die die Angreifer getrennt in Fehlerprotokollen aufbewahren wollen. Viele der Rückruf-URLs sind fehlerhaft, einige stammen aus unerwünschten IP-Adressbereichen, und bei anderen handelt es sich um eindeutig nicht erwünschte Rückrufe durch Sandbox-Systeme von Virenforschern.

Eine Beschreibung der einzelnen Connectback-URL-Werte und des zugehörigen xor/base64-Codierungsschemas finden Sie unter „Interesting Malware Trojan. Win32.Karba.e" in Anhang D.

Die Darkhotel-C&C-Server unterhalten die folgenden Verzeichnisstrukturen, um ddrlog-Inhalte zu speichern und zur Verfügung zu stellen:

- /bin/error/ddrlog
- /patch/error/ddrlog

Die folgenden Verzeichnisstrukturen scheinen sich bei allen Servern zu wiederholen, stellen jedoch kein ddrlog zur Verfügung und enthalten auch kein /error/-Verzeichnis:

- /u2/
- /u3/
- /patch2/
- /major/
- inor/
- /asp/
- /update3/

Zwei ddrlog-Dateieinträge beginnen am 1. Januar 2009 um 9:16.

- autozone.000space.com
- genuinsman.phpnet.us

Sämtliche Protokolldateien enthalten eine erhebliche Anzahl von Einträgen, fast 50.000, die jeweils mit einem einfachen Stempel, „B" oder „L" gekennzeichnet sind. Die Datensätze liegen im folgenden Format vor:

```
2009.01.01 09:16:00 150.70.xxx.xx --> B
2009.01.01 09:16:33 150.70.xxx.xx --> B
2009.01.01 09:14:52 220.108.x.xxx --> L
2009.01.01 09:16:04 112.70.xx.xx --> L
```

Bei nur 120 IP-Adressen wurde die „B"-Anmeldung ausgeführt, wobei 90 % der Adressen aus dem Adressbereich 150.70.97.x stammten. Der gesamte Bereich wurde für Trend Micro in Tokyo, Japan registriert.

Einige wenige der übrigen Adressen, z. B. 222.150.70.228, scheinen aus anderen Adressbereichen im Besitz von Trend Micro in Japan zu stammen. Einer der Ausreißer stammt von einem ISP in El Salvador, ein anderer von einem japanischen ISP. Bei ca. 20.000 IP-Adressen wurde die „L"-Anmeldung ausgeführt.

Andere ddrlogs enthalten u. a. den „A"-Stempel.

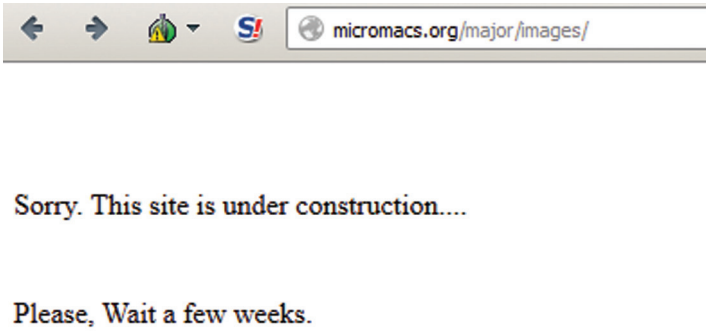
Dieser Stempel dient dazu, unerwünschte Anmeldungen aus nicht ins Visier genommenen Gebieten wie Ungarn oder Italien zu markieren. Der „B"-Stempel markiert unerwünschte Anmeldungen aus Trend Micro IP-Adressbereichen.

Der „L"-Stempel markiert unerwünschte Anmeldungen aus unterschiedlichen Adressbereichen, enthält jedoch auch merkwürdige IP-Adressen, z. B. die Loopback-Adresse 127.0.0.1, die eindeutig einen Fehler darstellt.

In den Protokolleinträgen sind außerdem Callback-URLs mit Leerzeichen und ungewöhnlichen Zeichen zu finden, die nicht aus dem vorgeschriebenen Base64-Zeichensatz stammen.

C&C-Kommunikation und -Struktur

Aussehen einer typischen Hauptseite:



Für „begatrendstone.com" konnte die folgende Verzeichnisstruktur ermittelt werden:

/bin
    -read_i.php (primäres C&C-Skript)
    -login.php (unbekannt, gibt „Wrong ID()" zurück)
/bin/error (hier gespeicherte Fehlerprotokolle)
    -ddrlog
/bin/tmp
 /bin/SElhxxwiN3pxxiAPxxc9
    -all.gif
    /i
    - verschlüsselte Inhalte von Zielsystemen
    /L
    /f

Für „auto2116.phpnet.us" konnte die folgende Verzeichnisstruktur ermittelt werden:

/patch

-chkupdate.php (primäres C&C-Skript)
/patch/error
-ddrlog

Die Gruppe verschlüsselt die von den Angriffszielen erbeuteten Daten mit einzelnen Benutzer-/Hauptschlüssel-Kombinationen für mehrere Angriffsziele. Versucht ein unbefugter Benutzer, ohne den korrekten Hauptschlüssel auf eine Darkhotel-Webseite zuzugreifen, um Zugang zu Daten von Angriffszielen zu erlangen, werden HTML-Seite und -Tabelle zwar korrekt dargestellt, die Daten werden aber als unleserlicher Chiffretext ausgegeben.

Umgang mit Angriffszielen

Die Systeme von potentiellen Angriffszielen werden offensichtlich systematisch ausgeforscht. Die Angreifer betreiben hierfür eine eigene Webseite. Die Zielsysteme werden dabei vor allem anhand ihrer aktuellen Anmeldung beim C&C-Server sortiert und bewertet. Die erfassten Daten werden wahrscheinlich nach ihrer Bedeutung sortiert dargestellt:

1. Anmeldename des Benutzers
2. CPU und Betriebssystem
3. „Ping sec" oder wie weit das Angriffsziel vom C&C-Server entfernt ist
4. „In": Der Prozess, in dem der DLL-Code des Angreifers ausgeführt wird
5. Vac: Kennung für Antivirenprodukt
6. System-LAN-IP
7. Netzwerk-WAN-IP

Hier ein Beispiel für eine dieser Webseiten:

Last connection	Information
0d 0h 2m 17s	Sys@User : [redacted] (0411) C P U : Intel(R) Pentium(R) M processor 1600MHz System OS: Microsoft Windows XP (Service Pack 3) Ping sec : [redacted]ms -> average [redacted]ms In : C:₩WINDOWS₩system32₩alg.exe Vac : Net card : [redacted] ([redacted]) Inter IP : [redacted]
0d 3h 10m 49s	Sys@User : [redacted] (0411) C P U : Intel(R) Core(TM) i7-2600K CPU @ 3.40GHz System OS: ₩indows 7 Professional () Ping sec : [redacted]ms -> average [redacted]ms In : c:₩program files (x86)₩uTorrent₩uTorrent.exe Vac : TR, Net card : [redacted] ([redacted]) Inter IP : [redacted]

Aktivität von Virenforschern

Zweifellos enthalten diese Protokolle auch eine Vielzahl von Einträgen, die auf die automatische Analyseaktivität von Virenforschern, z. B. durch Sandbox-Tools, zurückgehen. Im Zeitraum Juni 2013 bis April 2014 (also ca. 11 Monate) konnten in nur 15 ddrlog-Dateien nicht weniger als 7.000 Verbindungen durch derartige Sandbox-Systeme festgestellt werden. Über die durch die Netzwerkverbindungen gelieferten Werte „a1“= bis „a3=“ konnte eine QEMU-basierte Sandbox identifiziert werden. Alle Verbindungen konnten auf nur 485 WAN-IP-Adressen zurückgeführt werden. Es wurden weniger als 30 LAN-IPs aufgezeichnet, von denen alle aus demselben Bereich, 172.16.2.14-126, stammen. Für dieses System wird das Benutzerkonto „Dave” und der Windows-Systemname „HOME-OFF-D5F0AC” verwendet.

Diese Eigenschaften stimmen mit Netzwerkaktivität überein, die von GFI Softwares „CWsandbox”-Tools erzeugt wird, die mittlerweile Eigentum von „ThreatTrack Security” sind.

Fazit

In den vergangenen sieben Jahren hat ein leistungsfähiger Bedrohungsakteur namens Darkhotel, der auch als Tapaoux bekannt ist, eine Reihe erfolgreicher Attacken gegen unterschiedliche Angriffsziele auf der ganzen Welt ausgeführt. Die eingesetzten Methoden und Techniken gehen dabei weit über das typische Verhalten von Cyberkriminellen hinaus.

Darkhotel ist in der Lage, außergewöhnliche kryptografische Attacken auszuführen, beispielsweise die Faktorisierung von 512-Bit-RSA-Schlüsseln. Die Verwendung von Zero-Day-Exploits ist ein weiterer Hinweis auf einen leistungsstarken Bedrohungsakteur.

Gezielte Angriffe auf führende Mitarbeiter von Großunternehmen weltweit während ihres Aufenthalts in bestimmten „Dark Hotels" ist einer der interessantesten Aspekte dieser Operation. Die genaue Methode der Zielerfassung ist bislang immer noch nicht bekannt, z. B. die Frage, warum bestimmte Personen als Ziel ausgewählt werden und andere nicht. Der Umstand, dass es sich bei den meisten Opfern um Führungskräfte handelt, lässt vermuten, dass die Angreifer über den zeitweiligen Aufenthaltsort ihrer Angriffsziele, inklusive Name und Adresse der Unterkunft, im Voraus informiert sind. Hieraus ergibt sich das Bild eines undurchsichtigen und gefährlichen Netzes, in das sich nichts ahnende Reisende leicht verstricken können. Obwohl der genaue Grund, warum einige Hotels als Angriffsvektor fungieren, weiterhin unbekannt ist, gibt es bestimmte Vermutungen, die auf eine viel umfassendere Gefährdung hinweisen. Wir sind derzeit noch damit beschäftigt, diesen Aspekt der Operation zu untersuchen, und werden entsprechende Ergebnisse zu gegebener Zeit veröffentlichen.

Eine weitere interessante Eigenschaft ist die Nutzung unterschiedlicher Arten von Kampagnen, entweder gezielt oder per Botnet. Diese Vorgehensweise wird innerhalb der APT-Szene immer beliebter. Dabei werden gezielt hochrangige Opfer ins Visier genommen, während Botnet-Operationen dazu dienen, eine umfassende Überwachung zu gewährleisten oder andere Ziele zu verfolgen, z. B. Gegner durch DDoS-Attacken anzugreifen oder die Spionage-Tools auf Zielsystemen „hochzustufen".

Wir gehen davon aus, dass die Darkhotel-Gruppe auch weiterhin den Rüstungssektor, Behörden und nichtstaatliche Organisationen ins Visier nehmen wird. Im Anhang zu diesem Dossier finden Sie technische Gefährdungsindikatoren, die Opfern dabei helfen sollen, schädlichen Datenverkehr zu identifizieren und sich effektiver vor Attacken zu schützen.

Kaspersky Labs GmbH

Despag-Straße 3,
85055 Ingolstadt,
85055 Ingolstadt, Deutschland

weitere Kontaktdetails

Tel: +49 841 981 89 0
Fax: +49 841 981 89 100

E-Mail: info@kaspersky.de
Website: www.kaspersky.de