idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Ruhr-Universität Bochum
Dr. Julia Weiler
07/24/2019
http://idw-online.de/en/news719701

Research results
Economics / business administration, Information technology
transregional, national

Wirtschaftsspionage: Hackergruppe „Winnti“ hat mehrere deutsche Firmen im Visier

Wie die Hackergruppe „Winnti“, auch bekannt als APT10, deutsche und internationale Firmen attackiert und wer bereits unter den Opfern ist, haben Forscher der Ruhr-Universität Bochum gemeinsam mit einem Rechercheteam des Bayerischen Rundfunks und des NDR zutage gefördert. Winnti operiert vermutlich seit mindestens zehn Jahren aus China heraus und späht Unternehmen weltweit aus. In Deutschland wurden unter anderem Angriffe auf die Firmen Thyssen-Krupp und Bayer bekannt. Nach Analysen des Teams um Prof. Dr. Thorsten Holz vom Bochumer Horst-Görtz-Institut für IT-Sicherheit sind mindestens ein Dutzend Firmen von der Winnti-Software betroffen, darunter sechs Dax-Konzerne.

Besonders im Fokus stehen Unternehmen der chemischen Industrie, darüber hinaus aber auch Hersteller von Computerspielen, Telekommunikationskonzerne, Pharmaindustrie und die Halbleiterbranche. Die Medien berichteten am 24. Juli 2019 über die Ergebnisse der Recherche.

Schadsoftware aus dem Baukasten

Der Medienverbund von BR und NDR zog Thorsten Holz und seinen Doktoranden Moritz Contag zu der Recherche hinzu, weil sie Experten für die Analyse von Software, speziell Binärcode sind. Sie wollten genauer wissen, wie die Winnti-Spionage funktioniert. „Es gibt mittlerweile drei Generationen der Winnti-Software“, erklärt Thorsten Holz, einer der Sprecher des Exzellenzclusters Casa (Cyber-Security in the Age of Large-Scale Adversaries). „Die Software ist modular wie ein Baukasten aufgebaut. Daraus kann die Gruppe dann für den jeweiligen Zweck und die Opferfirma die passende Schadsoftware zusammensetzen.“

Der Baukasten enthält etwa ein Modul, das die Software auf einem Server des betroffenen Unternehmens versteckt, ein Modul, das das Sammeln von Informationen im Firmennetzwerk ermöglicht, oder ein Modul, das einen Kommunikationskanal nach draußen aufbaut.

Kontrollserver für Schadsoftware steht teils im Firmennetzwerk

Im Binärcode der Software ist auch eine Konfigurationsdatei enthalten, die entscheidende Optionen zur Steuerung der Schadsoftware enthält. Binärcode kann vom Prozessor direkt ausgeführt werden, ist aber für Menschen kaum verständlich. Die Bochumer IT-Experten übersetzten den Code in lesbare Sprache und zeigten, dass die Dateien beispielsweise die Information enthielten, von welchem Server aus die Schadsoftware gesteuert wurde und wo im Opfersystem die Schadsoftware liegt. Häufig nutzte die Hackergruppe externe Server zur Kontrolle, teilweise wurde die Schadsoftware aber auch von kompromittierten Servern im Firmennetzwerk gesteuert. „Interessanterweise enthalten die Konfigurationsdateien auch Hinweise, welche Firma oder Organisation konkret angegriffen wurde, erklärt Thorsten Holz. „Vermutlich hilft das der Gruppe, ihre Angriffe zu organisieren.“

Die analysierten Schadsoftware-Dateien stammten aus der Datenbank „Virustotal“. Bei diesem Dienst kann jeder beliebige Anwender Dateien hochladen und von 50 verschiedenen Virenscannern prüfen lassen. Alle hochgeladenen Dateien werden in einer Datenbank hinterlegt.

Moritz Contag analysierte mehrere Versionen der Schadsoftware und wertete mit dem gewonnenen Wissen mehrere hundert Konfigurationsdateien aus. Er konnte auch Zertifikate extrahieren, mit denen die Angreifer ihre Schadsoftware noch besser verstecken können.

Die Reporter kontaktierten insgesamt 14 Firmen, um sie auf die mögliche Infektion mit der Schadsoftware hinzuweisen. Einige der betroffenen Firmen räumten einen entsprechenden Angriff ein, teilweise laufen die Analysen noch. Unter den Betroffenen sind aber nicht nur Unternehmen; Winnti spionierte beispielsweise auch die Regierung Hongkongs aus. Die Medien vermuten daher, dass die Gruppe nicht nur Wirtschatfsspionage, sondern außerdem politische Spionage betreibt.

So werden Netzwerke infiziert

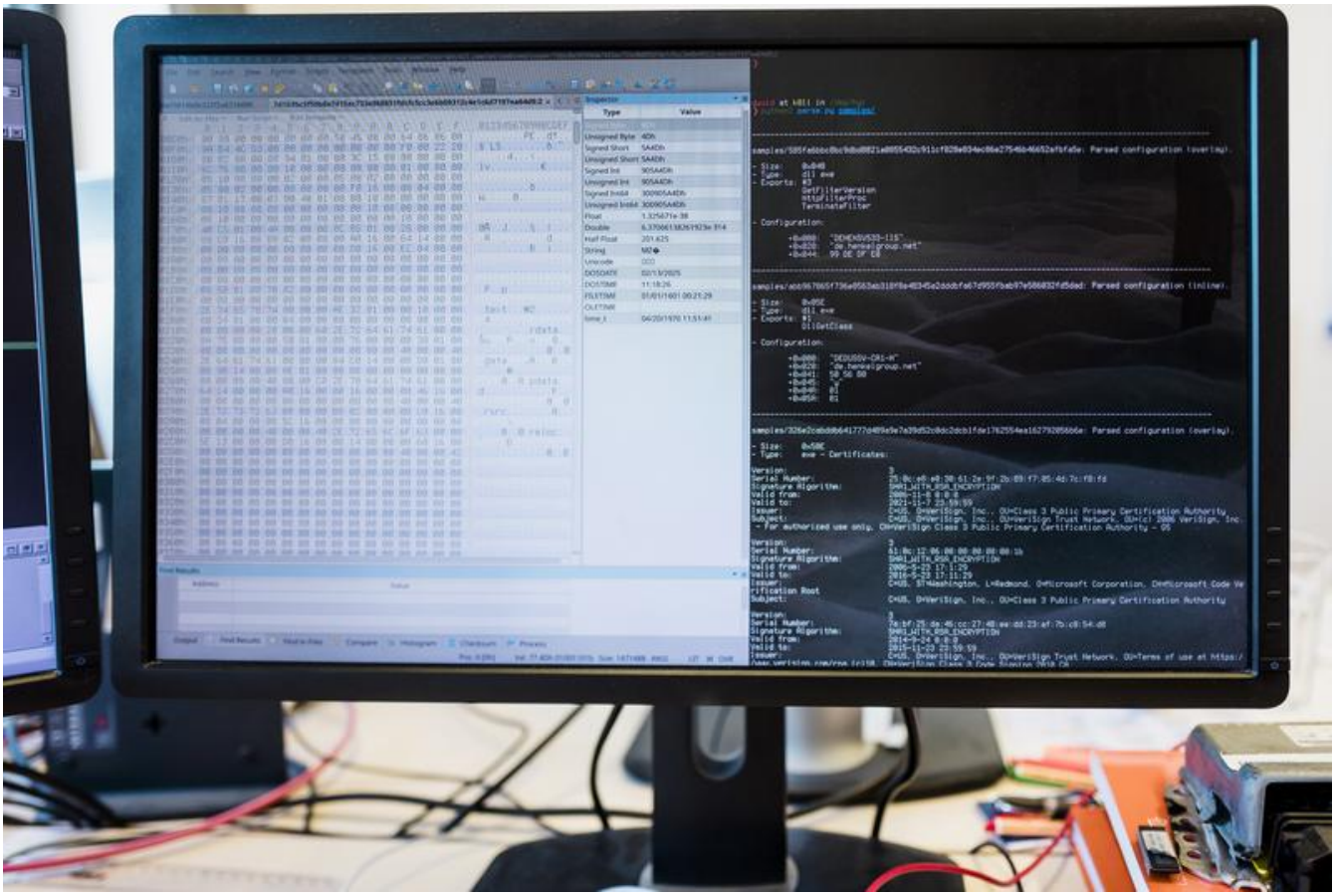
Die Infektion mit der Schadsoftware erfolgt häufig über Phishing-Mails. Klickt ein Nutzer auf einen Link in einer solchen Mail oder öffnet den Anhang, installiert sich die Winnti-Software auf dem System. Die Angreifer nutzen dieses System dann für weitere Angriffe innerhalb des Firmennetzwerks. Auf einem infizierten Server kann sich die Software unbemerkt verstecken, bis sie ein Signal vom Kontrollserver enthält und aktiviert wird. Dann kommuniziert das Programm über einen verschlüsselten Kanal mit dem Kontrollserver, sendet etwa bestimmte Daten aus dem Firmennetzwerk an die Angreifer.

„Wir haben in der Analyse auch gesehen, dass die Winnti-Software häufig wochen- oder monatelang schläft und nichts tut, dann für einen Tag oder auch mal eine Woche aktiviert wird, bevor sie wieder abgeschaltet wird“, beschreibt Thorsten Holz das typische Verhalten.

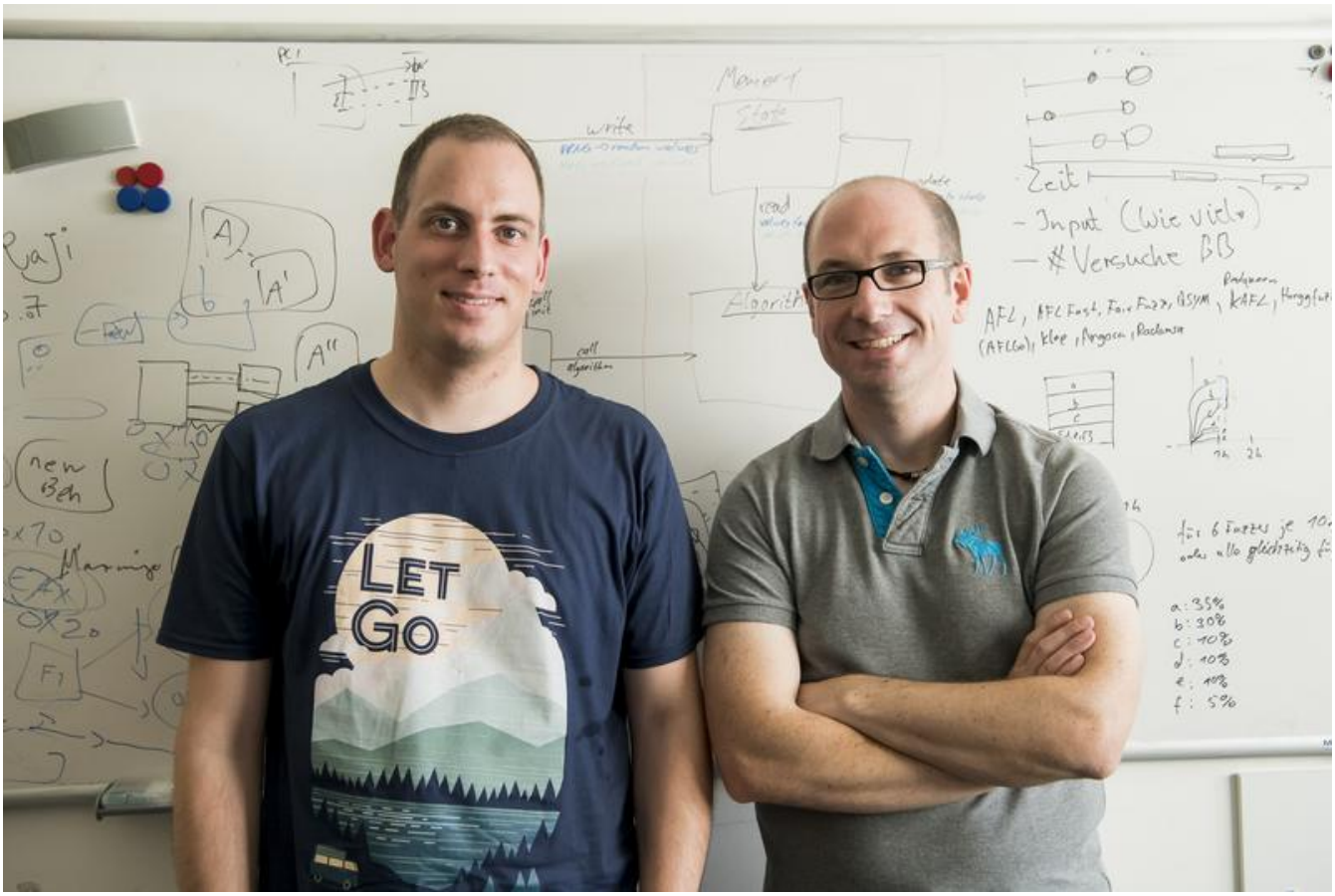
Angriffe mittlerweile auch auf Linux-Systeme

Die Winnti-Software hat zum Ziel, Systeme mit dem Windows-Betriebssystem zu infizieren. Inzwischen existiert auch eine Version für Linux, wie im März 2019 bekannt wurde. „Auch diese Version der Schadsoftware haben wir genauer unter die Lupe genommen“, so Thorsten Holz. „Sie funktioniert im Grunde genauso wie Winnti.“

contact for scientific information:
Prof. Dr. Thorsten Holz
Lehrstuhl für Systemsicherheit
Horst-Görtz-Institut für IT-Sicherheit
Ruhr-Universität Bochum
Tel.: 0234 32 25199
E-Mail: thorsten.holz@rub.de



Binärcode, hier im linken Fenster sichtbar, ist für Menschen nicht direkt lesbar. Teil der Arbeit der Bochumer Forscher ist es, den Code in verständliche Sprache zu übersetzen (rechts).



Prof. Dr. Thorsten Holz (rechts) und Moritz Contag vom Bochumer Horst-Görtz-Institut für IT-Sicherheit
© Mareen Meyer (Dieses Foto darf nur für eine Berichterstattung mit Bezug zur Ruhr-Universität Bochum im Kontext dieser Presseinformation verwendet werden.)