Angriff auf das Herz der deutschen Industrie

Seit Jahren spioniert eine professionelle Hackergruppe weltweit Unternehmen aus: Winnti. Mutmaßlich gesteuert aus China. Recherchen von BR und NDR zeigen erstmals das Ausmaß und wie die Hacker vorgehen. — von Hakan Tanriverdi, Svea Eckert, Jan Strozyk, Maximilian Zierer und Rebecca Ciesielski

English version: Our report on hackers for hire, conducting industrial espionage

Schadsoftware: Das können Computerviren sein oder aber Trojaner.

Die Recherche beginnt mit einem Code: `daa0 c7cb f4f0 fbcf d6d1` . Wer ihn kennt, kommt „Winnti“ auf die Schliche. Hackern, die seit Jahren

Reporterinnen und Reportern von BR und NDR ist es erstmals gelungen, Hunderte Varianten der dafür verwendeten Schadsoftware auszuwerten. Betroffen sind mindestens sechs Dax-Konzerne, Aushängeschilder der deutschen Industrie.

Winnti ist ein schwer zu durchdringender Komplex. Der Begriff bezeichnet einerseits eine ausgefeilte Schadsoftware, andererseits auch eine konkrete Gruppierung. IT-Sicherheitsexperten sprechen gar von einer digitalen Söldnertruppe. Mindestens seit 2011 setzen diese Hacker die Schadsoftware ein, um Unternehmensnetze auszuspionieren. Sie sammeln Informationen über die Organigramme von Firmen, welche Abteilungen zusammenarbeiten, über die IT-Systeme einzelner Firmenteile und natürlich auch Geschäftsgeheimnisse.

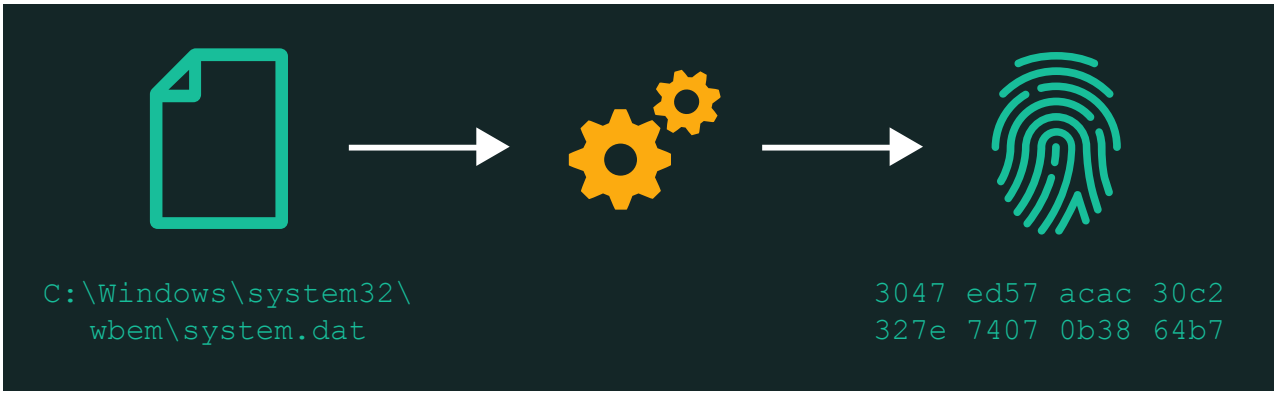
Ein IT-Sicherheitsexperte, der die Angriffe seit Jahren analysiert, sagt halb im Scherz: „Ein Dax-Konzern, der nicht von Winnti angegriffen wurde, hat irgendetwas falsch gemacht." Ein hochrangiger deutscher Beamter sagt: „Die Fallzahlen sind immens". Die Gruppe sei sehr aktiv – auch heute noch. Der Beamte bleibt namentlich ungenannt, ebenso wie der Großteil der mehr als 30 Personen, mit denen wir für diesen Artikel sprechen konnten: Firmen-Mitarbeiter, IT-Sicherheitsexperten, Regierungsbeamte und Vertreter von Sicherheitsbehörden. Offen sprechen wollen oder dürfen sie nicht. Doch Taktiken können sie preisgeben.

So können wir die Software finden und selbst sehen, wie die Angreifer arbeiten. Mit Hilfe der Informanten kommen wir, die Reporterinnen und Reporter, der Gruppe auf die Spur: Ein Teil dieser Spur ist der Code: `daa0 c7cb f4f0 fbcf d6d1` .

Protokoll: Die einzelnen Schritte der Hacker werden in Logdateien abgespeichert.

Moderne Spionageoperationen haben einen großen Vorteil: Anstatt Agenten in Unternehmen einzuschleusen, schicken digital arbeitende Spione eine präparierte E-Mail. Anstatt vertrauliche Unterlagen zu fotografieren, während die anderen Mitarbeiter in der Kantine sitzen, loggen sich Hacker aus der Ferne auf Unternehmensrechnern ein und schicken ihre Befehle per Tastatur. Doch die Hacking-Operationen haben auch einen Nachteil. Sie hinterlassen digitale Spuren. Wer die Hacker bemerkt, kann ihre Schritte protokollieren. Die Hacker

Um die Spuren der Hacker zu entschlüsseln, muss man sich den Programmcode der Schadsoftware selbst genauer ansehen. Finden kann man ihn zum Beispiel in von Privatfirmen betriebenen Datenbanken wie „Virustotal“. Die Firma gehört Google und ist eine Art Suchmaschine für Schadsoftware. Die dort hinterlegten Informationen sind für IT-Berater und Sicherheitsfirmen so wertvoll, dass der Zugriff tausende Euro im Monat kostet. Menschen, die sich nicht sicher sind, ob ein Mail-Anhang einen Trojaner enthält, können ihn hier von weit über 50 Antiviren-Programmen checken lassen. Im Gegenzug speichert Virustotal die Datei ab, mit Hilfe eines digitalen Fingerabdrucks. Mit dem können auch andere Menschen nach der Datei suchen und die dort enthaltenen Codes analysieren. Wir zum Beispiel.



Jede Datei hat einen digitalen Fingerabdruck – sie ist damit eindeutig identifizierbar.

Früher deckten ausschließlich Nachrichtendienste Spionage-Operationen auf. Heute beschäftigen Konzerne und IT-Sicherheitsfirmen Mitarbeiter mit sechsstelligen Jahresgehältern. Sie suchen in den Firmennetzen und auf Virustotal nach Hinweisen auf Hackergruppen. Denn ausspioniert werden schließlich die Konzerne, in denen sie arbeiten – und geheime Formeln und Baupläne müssen geschützt werden. Diese Mitarbeiter können es fachlich mit den Diensten aufnehmen. Es ist so eine Person, die sich mit uns trifft und ein Blatt Papier über den Tisch schiebt.

„Damit könnte man die Hacker finden“, sagt der Mann. Denn sie spionieren sehr viele Ziele gleichzeitig aus und müssen deshalb einen Weg finden, um den Überblick zu behalten. Dabei hätten sie auf Bequemlichkeit gesetzt statt auf Anonymität. Schon bald merken wir, wie erstaunlich fahrlässig die Hacker vorgehen. Wir arbeiten mit Moritz Contag zusammen, einem IT-

direkt in ihre Schadsoftware. Contag hat über 250 Varianten der Winnti-Schadsoftware analysiert und darin Namen von Weltkonzernen gefunden.

Opsec: Operational Security. Sammelbegriff für alle Schritte, die Hacker unternehmen, um ihre Spuren zu verwischen.

Hacker treffen normalerweise Vorsichtsmaßnahmen, Fachleute sprechen von Opsec. Bei der Winnti-Gruppe war sie miserabel. Vielleicht war es ihnen nicht so wichtig, vermutet jemand, der für einen europäischen Nachrichtendienst chinesische Hacker im Blick behielt: „Diesen Hackern ist egal, ob sie erkannt werden. Sie wollen nur ihre Ziele erreichen."

Auf dem Blatt Papier, das der Mitarbeiter uns zeigt, steht der Code `daa0 c7cb f4f0 fbcf d6d1`. Diese Zeichenfolge finden wir auch bei Virustotal wieder, der gigantischen Datenbank mit infizierten Dateien.

`c7cb f4f0 fbcf d6d1` . In diesem Datenstrom verstecken die Winnti-Hacker ihre Befehle.

Schritt 2: Die Daten sind leicht zu demaskieren. Ab jetzt können wir sehen, was die Hacker vorhaben. `daa0 c7cb f4f0 fbcf d6d1`

Schritt 3: Damit die Hacker wissen, in welchem Netzwerk sie sich befinden, schreiben sie es einfach direkt in ihr Programm. In diesem Beispiel sind die Winnti-Hacker in den Netzwerken von `Gameforge`.

```
daa0  c7cb  f4f0  fbcf  d6d1  ffd7  dcd5  d3cd  c499  99f0  dacc  cadd
edc1  cac7  c1d3  da96  dddb  cfbc  bdbe  bfc0  c1c2  c3c4  c5c6  c7c8
999a  9b9c  eafc  facd  c2cd  ceca  8bc2  cbc4  a9aa  abac  adae  afb0
b1b2  b3b4  b5b6  b7b8  b9ba  bbbc  cec7  ccb4  a4af  eda6  aca8  c7c8
c9ca  cbcc  cdce  cfd0  d1d2  d3d4  d5d6  d7d8  f9fa  fbfc  fdfe  ff00
0102  0304  0506  0708  090a  0b0c  0d0e  0f10  1112  1314  1516  1718
191a  1b1c  1d1e  1f20  2122  2324  2526  2728  292a  2b2c  2d2e  2f30
3132  3334  3536  3738  393a  3b3c  3d3e  3f40  2521  4344  4546  4748
595a  5b5c  5d5e  5f60  0603  0e01  0309  150f  0c6a  6b6c  6d6e  6f70
7172  7374  7576  7778  797a  7b7c  7d7e  7f80  b1b5  b2b3  8586  8788
                898a  8b8c  8d8e  8f90  9192  9394
```

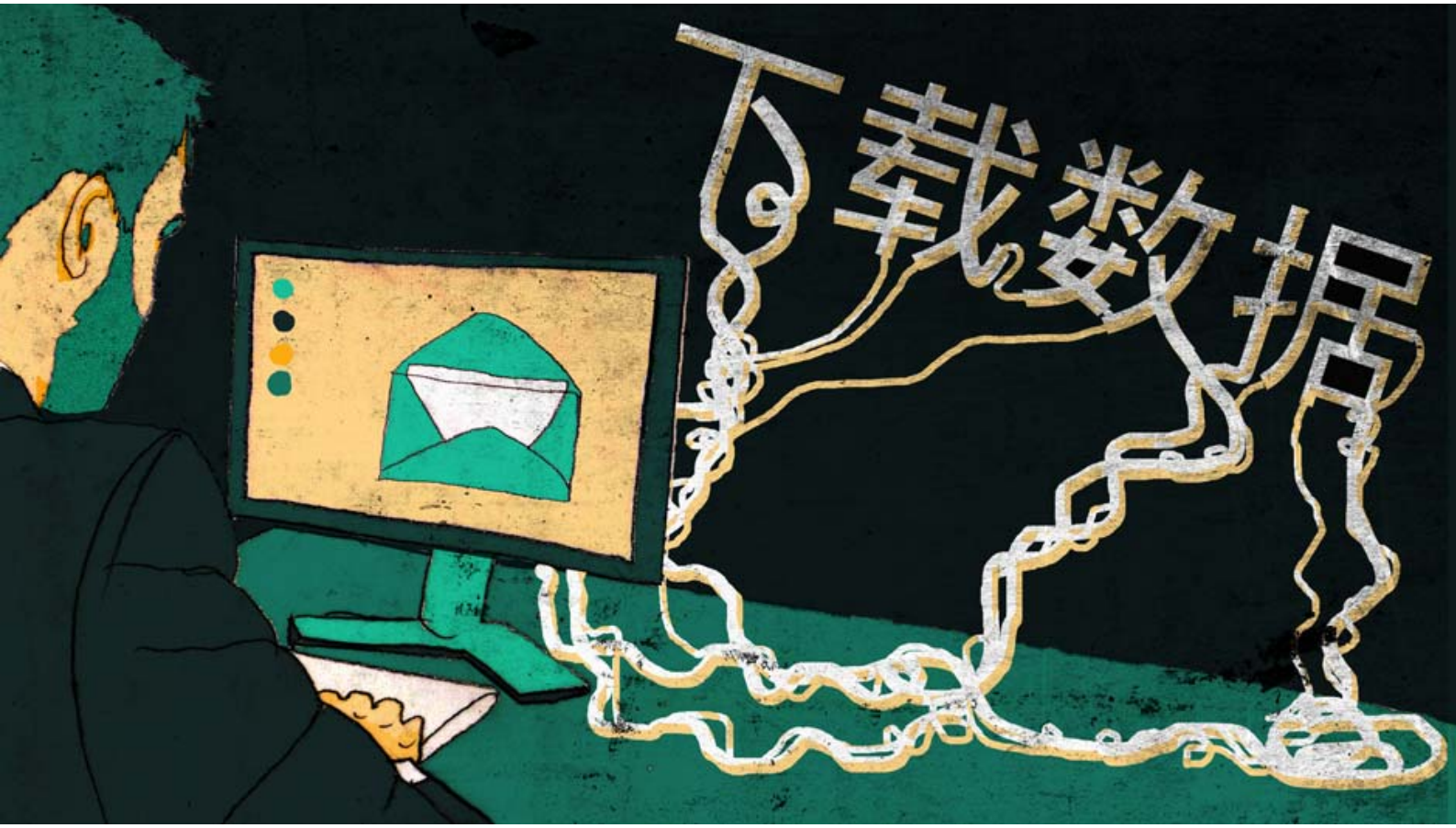
Phase 1: Cyberkriminalität

In der Anfangsphase ging es den Hackern anscheinend darum, Geld zu verdienen. Das zeigt der Fall `Gameforge` : eine Spiele-Firma mit Sitz in Karlsruhe. In den besten Jahren des Unternehmens arbeiteten hier 700 Mitarbeiter daran, den Gaming-Markt weltweit zu erobern, der Umsatz lag bei rund jährlich 140 Millionen Euro. Gameforge bietet so genannte „Freemium“-Spiele an. Gezockt wird kostenlos, wer mehr will, muss sich virtuelles Geld

Im Jahr 2011 landet nach unseren Informationen eine E-Mail im Gameforge-Postfach in Karlsruhe. Ein Mitarbeiter öffnet die angehängte Datei und startet damit, ohne dass er es weiß, das Winnti-Programm der Hacker. Kurz darauf werden einige Spieler virtuell reich.

Die Administratoren sehen, dass jemand die Datenbanken direkt ansteuert und dort den Kontostand nach oben schraubt. Sie werden nervös. Das kann eigentlich nicht sein. Die nächsten Wartungsarbeiten nutzen die Techniker, um die Server des betroffenen Spiels neu zu installieren. Die Spieler ahnen nichts. Doch kaum laufen die Server wieder, wird weiter manipuliert.

Gameforge setzt Antiviren-Software von Kaspersky ein. Die schlägt keinen Alarm. Also holt man die IT-Sicherheitsexperten direkt nach Karlsruhe. Denn es ist offensichtlich, dass etwas nicht stimmt. Das Landeskriminalamt oder die örtliche Polizei informiert niemand. Es ist 2011, und Cyberkriminalität ist für viele Ermittler ein Wort, das ihnen noch nicht so leicht über die Zunge rollt.



Hacker im System sind – und sich die meiste Zeit so benehmen wie die Administratoren von Gameforge. Dadurch waren sie unsichtbar. Insgesamt 40 Server haben die Hacker übernommen.

Persistent: Es ist sehr schwer die Hacker aus dem Netzwerk zu entfernen.

Es ist ein Vorgehen, das typisch ist für viele Hackergruppen – aber insbesondere für Winnti. „Das ist eine sehr, sehr persistente Gruppe“, sagt Costin Raiu, der Winnti seit 2011 beobachtet. Raiu leitet bei Kaspersky das Team, das Schadsoftware analysiert. „Sobald die Winnti-Hacker im Netz sind, lassen sie sich sehr viel Zeit, um die Infrastruktur zu verstehen“, sagt er.

Die Hacker kartieren zum Beispiel das Unternehmens-Netzwerk, suchen strategisch günstige Punkte, um dort ihre Schadsoftware zu platzieren. Sie halten fest, welche Programme in einem Unternehmen verwendet werden und tauschen dann dort eine Datei aus. Sie arbeitet wie das Original, wurde aber tatsächlich heimlich um ein paar Codezeilen ergänzt. Diese manipulierte Datei gehorcht den Angreifern.

> **Winnti ist sehr speziell für Deutschland. Es ist die Angreifergruppe, die am häufigsten aufgetaucht ist.**
>
> Anonymer Behördenmitarbeiter

Raiu und sein Team verfolgten die digitalen Spuren, die einzelne Winnti-Hacker hinterließen. „Vor neun Jahren war die Situation viel klarer. Es gab ein Team. Das hat Winnti entwickelt und benutzt. Heute hingegen sieht es so aus, als ob mindestens eine zweite Gruppe existiert, die ebenfalls Winnti einsetzt.“ Viele IT-Sicherheitsfirmen teilen diese Ansicht. Und es ist diese zweite Gruppe, die deutschen Sicherheitsbehörden große Sorgen bereitet. Ein Behördenmitarbeiter formuliert es nüchtern: „Winnti ist sehr speziell für Deutschland. Es ist die Angreifergruppe, die am häufigsten aufgetaucht ist.“

Phase 2: Industriespionage

Die Hacker haben es auf Hochtechnologie-Unternehmen abgesehen, außerdem auf Chemie- und Pharmakonzerne. Wir finden Belege, die bis Mitte 2019 reichen. Spionagefälle, die wahrscheinlich noch laufen, während wir recherchieren. Winnti greift Unternehmen in Japan an, in Frankreich, in den USA und in Deutschland. Genauer: in Düsseldorf.

Den meisten Menschen ist der Dax-Konzern Henkel wohl vor allem als Hersteller von Waschmittel und Shampoo bekannt. Daneben bietet Henkel eine ganze Palette an anderen Produkten, unter anderem Klebstoffe für die Industrie. Moderne Autos werden geklebt statt geschweißt. In einem Werbeclip auf Youtube zeigt der Konzern, wie es Mitarbeitern gelang, zwei Metallplatten mit nur drei Gramm Klebstoff fest zu verbinden und dann einen 280-Tonnen schweren Zug zu ziehen. Rund die Hälfte des jährlichen Umsatzes von 20 Milliarden Euro geht auf den Bereich zurück, der bei Henkel „adhesive technologies“ genannt wird.

Die Winnti-Hacker drangen im Jahr 2014 in das Netz bei Henkel ein. Uns liegen drei Dateien vor, aus denen das hervorgeht. In diesen findet sich sowohl immer dieselbe Webseite, die Henkel gehört, als auch der Name der jeweils gehackten Server. Einer beginnt zum Beispiel mit der Buchstabenfolge DEDUSSV. Server können beliebig benannt werden, doch es liegt nahe, dass DE für Deutschland steht und DUS für Düsseldorf, dort liegt die Firmenzentrale. Die Hacker konnten sämtliche Aktivitäten überwachen, die über den Webserver liefen. Sie konnten wohl auch Systeme erreichen, die nicht direkt mit dem Internet kommunizierten: Interne Datei-Ablagen oder das Intranet womöglich.

Der Konzern bestätigt den Winnti-Vorfall und schreibt in einem Statement: „Die Cyber-Attacke wurde im Sommer 2014 entdeckt, und Henkel hat schnell alle notwendigen Maßnahmen eingeleitet.“ Ein „sehr kleiner Teil“ der weltweiten IT-Systeme sei betroffen gewesen – die Systeme in Deutschland. Es gebe keine Hinweise darauf, dass sensible Daten ausgeleitet worden seien.

Über die Recherche

allem Moritz Contag von der Ruhr-Universität Bochum hat aus verschiedenen Varianten der Schadsoftware Informationen extrahiert. Für diese Analyse hat Contag ein Skript geschrieben. Wir veröffentlichen es hier. Silas Cutler, IT-Sicherheitsexperte bei der US-Firma Chronicle Security hat die Analysen von Contag bestätigt.

Eine Kooperation von und

Winnti greift Henkel und die anderen Firmen nicht willkürlich an, sondern geht strategisch vor. Das zeigen die anderen Fälle. Da ist zum einen Covestro, das Unternehmen stellt ebenfalls Klebstoffe her, außerdem Lacke und Farben. Der Chemie-Konzern gehörte einst zu Bayer, wurde dann ausgegliedert und ist heute im Dax verzeichnet. Covestro wird als erfolgreichste Unternehmensabspaltung Deutschlands in der jüngeren Zeit gehandelt. Bis in den Juni 2019 hinein fanden sich mindestens zwei Systeme, auf denen die Winnti-Schadsoftware installiert war. Auch wenn es keine konkreten Hinweise für einen Datenverlust gebe, betrachtet Covestro „die vorgefundene Infektion als schwerwiegenden Angriff auf unser Unternehmen“. Ein weiterer Klebstoff-Hersteller, Bostik aus Frankreich, war Anfang 2019 von Winnti betroffen.

Auch auf das größte Chemieunternehmen aus Japan haben es die Hacker hinter Winnti abgesehen – Shin-Etsu Chemical. Mehrere mutmaßlich für die digitale Spionage eingesetzte Varianten der Schadsoftware aus dem Jahr 2015 liegen uns vor. Bei einem anderen japanischen Hochtechnologie-Konzern, Sumitomo Electric, gelangen die Hacker im Sommer 2016 in die Systeme. Und Roche, eines der größten Pharmaunternehmen der Welt: Ganze 25 Dateien geben eine Ahnung davon, an wie vielen Stellen sich die Hacker im Netz festgesetzt haben müssen. Und auch im Fall von BASF und Siemens drangen Winnti-Hacker in die Netze ein. Beide Konzerne bestätigen unsere Recherchen.

Eine BASF-Sprecherin teilt per Mail mit, dass es den Hackern im Juli 2015 gelungen sei, „die ersten Ebenen“ der Verteidigung zu überwinden. „Als unsere Experten feststellten, dass der Angreifer versuchte, die nächsten Verteidigungsebenen zu überwinden, wurde der Angreifer sofort und

Hacker im Juni 2016 ein, wie das Unternehmen angibt. „Der Angriff wurde von uns zügig erkannt und bewältigt“, heißt es in einer schriftlichen Antwort. Man habe nach ausführlichen Analysen bis heute keine Hinweise darauf, dass bei dem Angriff Daten abgeflossen seien.

Unternehmen im Visier

- **Gaming**: Gameforge, Valve
- **Software**: Teamviewer
- **Technologie**: Siemens, Sumitomo, Thyssenkrupp
- **Pharma**: Bayer, Roche
- **Chemie**: BASF, Covestro, Shin-Etsu

Die Unternehmen Bostik, Sumitomo und Shin-Etsu reagieren nicht auf unsere Fragen. Roche bleibt allgemein: Ein Unternehmenssprecher antwortet, dass man „Informationssicherheit und den Datenschutz sehr ernst“ nehme. Fast alle Großkonzerne betonen mittlerweile, dass es keinen hundertprozentigen Schutz geben kann. Hackerangriffe bei Großunternehmen sind mittlerweile alltäglich. Und doch: So wirklich gern redet kein Unternehmen darüber, Hacker in den eigenen Netzen zu haben. In den meisten Fällen werden die Kunden nicht informiert. Gefürchtet wird ein Reputationsschaden.

Das zeigt der Fall Teamviewer. Eine Firma aus dem südwestdeutschen Mittelstandsgürtel, die es mit der Konkurrenz aus dem Silicon Valley aufnehmen kann, ein Vorzeige-Unternehmen. Schnell wurde es mit einer Milliarden-Bewertung gehandelt, eine Art Ritterschlag unter Gründern. Dann kamen die Winnti-Hacker. Der „Spiegel“ berichtete darüber zuerst.

Der Konzern bietet eine Software-Lösung zur Fernwartung an, die nach Firmenangaben auf zwei Milliarden Geräten installiert ist. Der Schaden, den ein Hacker anrichten könnte, wenn ihm über die Teamviewer-Anwendung der

habe die komplette IT-Infrastruktur ausgetauscht, Millionen ausgegeben und die Hacker 2016 aus den Netzen entfernt.

Der zweite Weg zu Winnti

Für IT-Abteilungen sind die infizierten Rechner nur extrem schwer zu entdecken. Denn eine neue Variante der Schadsoftware bleibt passiv, solange sie in Ruhe gelassen wird. Wie soll man etwas finden, das sich tot stellt? Seit 2018 existiert ein öffentliches Werkzeug, das das Internet gezielt nach diesen infizierten Systemen durchpflügt. Dieser Netzwerkscan lockt die Software aus der Deckung.

Jede Firma hat einen eigenen IP-Adressbereich. Die IP-Adresse ist die eindeutige Adresse eines Rechners. Damit ist er über das Internet erreichbar.

Hat die Schadsoftware Winnti einen Computer infiziert, verhält sie sich zunächst passiv. Winnti wartet jetzt auf Steuerbefehle.

Mit Hilfe einer speziellen Software versenden wir Anfragen an verschiedene Firmennetze. Die Software ist harmlos, kann aber Steuerbefehle simulieren und damit Winnti aus der Deckung locken.

Ist Winnti installiert, antwortet die Schadsoftware auf unsere Anfrage. Damit wissen wir: Die Firma wurde gehackt.

Mitgezählt? Bis hierher sind zehn Unternehmen betroffen, größtenteils in Deutschland.

Dieses Werkzeug wird bei Covestro und bei Bostik fündig. Viele IT-Firmen gehen denselben Weg, um Winnti-infizierte Computer zu finden, ein paar der Ergebnisse werden uns zugespielt – unter strikter Vertraulichkeit. Denn mit diesem Werkzeug fanden wir bereits im März 2019 heraus, dass der Pharmakonzern Bayer von Winnti gehackt wurde.

Das Werkzeug geschrieben haben Mitarbeiter von Thyssenkrupp, denn auch der Industrie-Gigant – Unternehmen Nummer elf – ist von Winnti ausspioniert worden. 2016 erlaubte der Konzern einem Reporter der „Wirtschaftswoche“ dabei zu sein, wie die Angreifer zurückgedrängt wurden. Von einer „sechsmonatigen Abwehrschlacht“ schrieb das Magazin später. Den Hackern gelang es, kleinere Datensätze abzuziehen, die für den Bau von Anlagen wichtig sind. Der Konzern spricht von „Datenfragmenten“ und ist der Ansicht, dass die Hacker ihr eigentliches Ziel – das Abgreifen von Forschungsergebnissen – verfehlt hätten.

Die Spur nach China

auf. Vermutlich verwendeten die Hacker Werkzeuge in ihrer Sprache, das erleichterte ihnen die Arbeit. Sie vergaßen jedoch, diese Spur zu verwischen. Ein Fehler, der ihnen unterlaufen ist; einer von vielen.

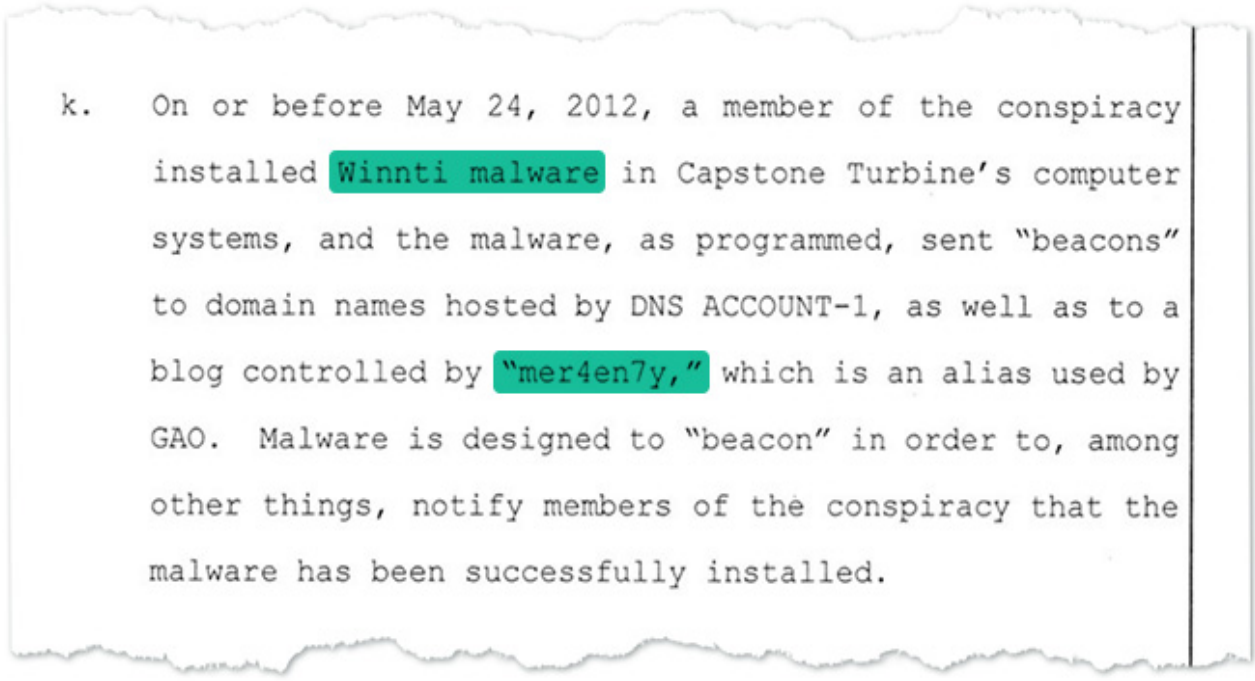
Mehrere Dax-Konzerne, darunter auch BASF und Bayer, haben im Oktober 2016 die Deutsche Cybersicherheitsorganisation (DCSO) gegründet. Der Job der IT-Sicherheitsexperten ist es, Hackergruppen wie Winnti zu beobachten, zu erkennen und auch über ihre Motive nachzudenken. Dror-Jöhn Röcher leitet das operative Geschäft bei der DCSO und spricht im Fall von Winnti von einer „Söldnertruppe“, die dem chinesischen Staat nahestehen soll. Man beobachte die Truppe schon sehr lang, „so dass wir aus ganz vielen Indizien sagen können, dass Winnti mit einer hohen Wahrscheinlichkeit chinesisch beziehungsweise chinesisch gesteuert ist.“ Zahlreiche Experten, mit denen wir sprechen, gehen davon aus, dass die Gruppe aus China heraus operiert. „Ob die Hacker nun in grünen Uniformen arbeiten oder aber von Leuten beauftragt werden, die grüne Uniformen tragen, ist mir egal“, sagt ein IT-Sicherheitsexperte und spielt damit auf eine vermutete Nähe zu dem militärischen Geheimdienst des Landes an.

> **Mit einer hohen Wahrscheinlichkeit ist Winnti chinesisch beziehungsweise chinesisch gesteuert**
>
> Dror-John Röcher, DCSO

Anfangs gingen die Winnti-Hacker offenbar noch unvorsichtig vor. Einer von ihnen hinterließ viele Spuren im Internet. Das Team von Kaspersky folgte 2013 Hinweisen im Code. So stießen Costin Raiu und seine Kollegen auf eine Person mit dem Alias „Mer4en7y“. Die Person war in Hacker-Foren aktiv und kommentierte dort auf Chinesisch ein Jobangebot, mit dem Hacker rekrutiert werden sollten. Von einem "mächtigen Hintergrund" war dort die Rede. „Und ‚Mer4en7y‘ hat geantwortet, dass ihm der Arbeitsplatz zu weit weg sei, er die Arbeit aber unterstütze“, sagt Raiu.

Am 30. Oktober 2018 erhebt die US-Regierung Anklage gegen zehn chinesische Staatsbürger. Zwei davon sollen für einen der Nachrichtendienste Chinas arbeiten. Den Hackern wird vorgeworfen, einen Hersteller von Gasturbinen ausspioniert zu haben. Mitangeklagt: „Mer4en7y“, der im Auftrag des

chinesische Gruppe zurück. Doch die Anklage belegt die Nähe, die zwischen mindestens einem Winnti-Hacker und dem Staat besteht.



k. On or before May 24, 2012, a member of the conspiracy installed Winnti malware in Capstone Turbine's computer systems, and the malware, as programmed, sent "beacons" to domain names hosted by DNS ACCOUNT-1, as well as to a blog controlled by "mer4en7y," which is an alias used by GAO. Malware is designed to "beacon" in order to, among other things, notify members of the conspiracy that the malware has been successfully installed.

Die US-Regierung wirft der Person mit dem Alias „Mer4en7y" vor, die Winnti-Software eingesetzt zu haben.

Janka Oertel arbeitet in Berlin für die US-amerikanische Stiftung German Marshall Fund und befasst sich mit der Außenpolitik des Einparteienstaates. Oertel hält es für „sehr unwahrscheinlich, dass großangelegte Cyber-Operationen ohne Kenntnis zumindest von Teilen des chinesischen Partei-Staats durchgeführt werden könnten." Die Politikwissenschaftlerin betont, dass China in Schlüsselindustrien wie zum Beispiel der Materialforschung bis 2025 eine „signifikante Marktrolle" einnehmen und bis 2035 weltweit dominieren will. „In einigen dieser Bereiche ist China aber durchaus noch nicht in der Lage, dies ohne Technologietransfer – auch aus Deutschland – zu erreichen", sagt Oertel.

Ein Behörden-Mitarbeiter, der die Hacking-Fälle kennt, stimmt zu: „Cyber-Vorfälle lassen Rückschlüsse darauf ziehen, worauf eine Nation Prioritäten setzt". Man müsse die eigene Industrie verstehen und merken, was nicht schnell genug produziert werden könne. In Hacking-Operationen werde dieses Material dann beschafft.

Doch ein Ex-Mitarbeiter eines europäischen Nachrichtendienstes warnt: „Wenn ich heute jemanden hacken würde, dann würde ich es genauso aussehen lassen

Aus deutschen Sicherheitskreisen heißt es: Alle bisherigen Erkenntnisse sprächen dafür, dass Winnti aus dem chinesischen Raum komme. Allerdings beruhe ein Großteil der Beweisführung auf Daten, die mehrere Jahre alt seien. Deshalb sei man vorsichtig. „Für die vergangenen zwei bis drei Jahre klafft eine Wissenslücke", sagt eine mit den Vorgängen betraute Person.

> **Wenn ich heute jemanden hacken würde, dann würde ich es genauso aussehen lassen wie eine chinesische Gruppe.**
>
> Ex-Mitarbeiter eines europäischen Geheimdienstes

Deutschland thematisiert Industriespionage in direkten Gesprächen mit der chinesischen Führung, wertet diese Versuche aber als vergebene Mühe. „Fruchtlos", wie einer sagt, der weiß, wie solche Treffen ablaufen. Die Gegenseite streite alles ab, am Ende komme nicht viel mehr heraus als nichtssagende Absichtserklärungen. Und die Deutschen wollen der chinesischen Führung auch nicht zu viel zu verraten – zum Beispiel durch die Arbeit des Bundesnachrichtendienstes (BND).

anderem bekommen, um ein mächtiges Überwachungs-System aufzubauen. Finden will man Hackergruppen, hinter denen ein Staat vermutet wird und die der Bundesrepublik Schaden zufügen könnten. Es wird ebenfalls überlegt, chinesische Angreifergruppen „offensiv aufzuklären". Das heißt: Sich in die Netze einzuhacken. Spione, die Spione beobachten.

Politische Spionage?

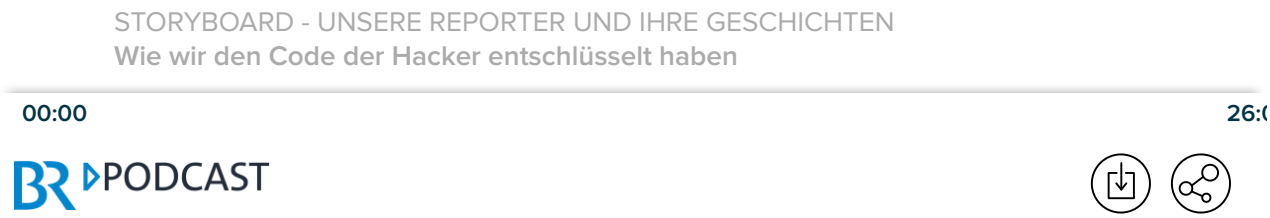
Konzerne wie Bayer, Covestro, Roche und Bostik verbindet der gemeinsame Sektor: die chemische Industrie. Die Analyse zeigt aber auch eine Reihe von Zielen die von dem bisherigen Muster stark abweicht. Es scheint sich um politische Spionage zu handeln. Dafür sprechen mehrere Hinweise, auf die wir gestoßen sind.

Die Regierung Hongkongs wurde von den Winnti-Hackern ausspioniert. Mit dem Netzwerkscan finden wir vier infizierte Systeme und informieren die Regierung per Mail. Diese bestätigt unsere Ergebnisse: Insgesamt auf sechs Rechnern von zwei Behörden sei die Winnti-Schadsoftware gefunden worden. „Auf den betroffenen Rechnern befanden sich weder als geheim eingestufte Informationen noch Daten von Bürgern", teilt man uns per Mail mit. Daten seien keine abgeflossen. Auch bei einem Telekommunikationsanbieter aus Indien schlägt der Netzwerkscan an, ausgerechnet in der Region, in der die tibetische Exil-Regierung („Central Tibetan Administration") ihren Hauptsitz hat. Die dazugehörige Kennung in der Schadsoftware lautet dementsprechend „CTA". In einer Datei, die 2018 auf Virustotal landet, steht ganz unverblümt „tibet". Die Exilregierung beantwortet unsere Anfragen nicht.

Hinzu kommen Kampagnen, bei denen schwerer zu verstehen ist, welche Motivation die Hacker antreiben sollte, wenn nicht politische Spionage. Da ist zum Beispiel Marriott, die Hotel-Kette aus Maryland, USA. Mehr als eine Million Zimmer verwaltet die Gruppe weltweit. Die Hotels mögen zwar modern sein, aber würde man Marriott hacken wollen, um Technologien oder innovative Ideen zu erbeuten? Würde man die indonesische Fluggesellschaft Lion Air aus diesen Gründen ausspionieren? Vermutlich nicht. Hotels und Fluglinien sammeln Daten. Wer sie einsehen kann, weiß, wohin Menschen reisen und wo

Telekommunikationskonzernen ist es den Winnti-Hackern gelungen, in das Netz einzudringen, Marriott hatten sie zumindest im Visier. Die entsprechend codierte Datei liegt uns vor. Weder Marriott noch Lion Air wollten sich äußern.

Podcast: Wie wir den Code entschlüsselt haben



Winnti: Eine Schadsoftware, die seit Jahren eingesetzt wird. Die Hacker müssen bislang wenig befürchten. IT-Sicherheitsexperte Röcher von der DCSO sagt, dass sich Sicherheitsbehörden, Ermittler und die Wirtschaft koordiniert austauschen sollten: „Und die Politik ist in der Verantwortung den Rahmen zu schaffen, dass das funktioniert."

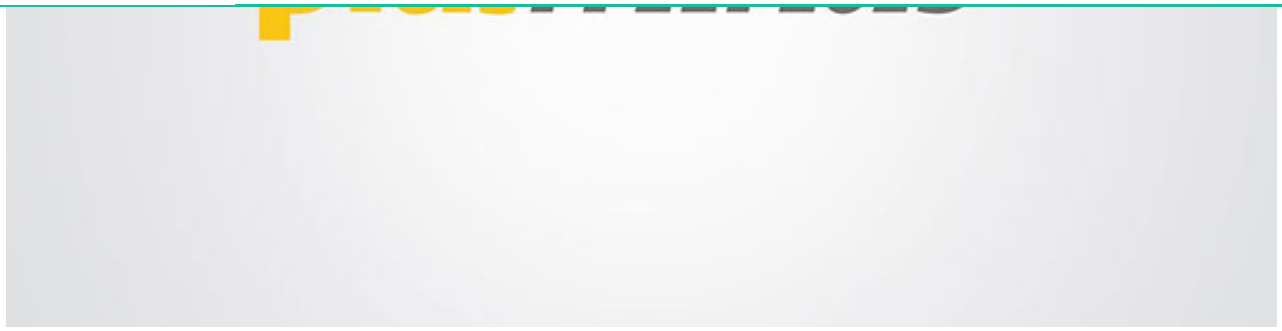
Auf Anfrage teilt das Bundesinnenministerium mit, dass die Sicherheitsbehörden zu diesem Zweck „verschiedene Plattformen und Gesprächsformate" anbieten würden. Bei Bedarf gebe man den betroffenen Unternehmen „geeignete Empfehlungen und Hilfestellungen zur Bereinigung und zukünftigen Prävention". Im Juli 2019 habe das BSI ein Unternehmen informiert, dessen Name in einer Schadsoftware enthalten war. Generell gelte: „Cyberangriffe haben sich als wichtige Methode der Informationsgewinnung für ausländische Nachrichtendienste fest etabliert". Ernsthafte politische oder strafrechtliche Risiken bestünden für die Hacker nicht, „aufgrund vielfältiger Verschleierungsmöglichkeiten."

Die Frage danach, ob es einen Zusammenhang zwischen den Winnti-Hackern und der chinesischen Regierung gibt, beantwortet das Ministerium ausweichend. Man nehme solche Vorfälle ernst, unabhängig vom Ursprung. Wir richten diese und andere Fragen an das chinesische Außenministerium und die chinesische Botschaft in Berlin – eine Antwort bekommen wir nicht.

Mehr zum Thema:

Tagesschau.de: Industriespionage: Mehrere Dax-Firmen von Hackerangriff betroffen

Der Funkstreifzug: Hackerangriffe auf deutsche Dax-Unternehmen



Plusminus: Deutsche Unternehmen stärker im Visier von Industriespionen (Mai 2019).

Über das Projekt

„Winnti: Angriff auf das Herz der deutschen Industrie" ist eine Recherche des Bayerischen Rundfunks (BR Recherche/BR Data) und des Norddeutschen Rundfunks.

Veröffentlicht am 24.07.2019

Autoren: Hakan Tanriverdi, Maximilian Zierer, Rebecca Ciesielski (BR), Svea Eckert, Jan Lukas Strozyk (NDR)
Mitarbeit: Maximilian Richt (BR)
Redaktion: Uli Köppen, Verena Nierle, Robert Schöffel
Illustrationen: Anna Hunger
Digitales Design: Steffen Kühne