

[Das ist Krieg: Die Ukraine wurde von der größten Cyberattacke ihrer Geschichte erschüttert](#)

28.06.2017

Am 27. Juni startete in der Ukraine gegen Mittag eine massive Cyberattacke, die mithilfe einer modifizierten Version des Virus „WannaCry“ – Petya.A ausgeführt wurde und mindestens einen Monat lang vorbereitet wurde.

Am 27. Juni startete in der Ukraine gegen Mittag eine massive Cyberattacke, die mithilfe einer modifizierten Version des Virus „WannaCry“ – Petya.A ausgeführt wurde und mindestens einen Monat lang vorbereitet wurde.

Die E-Mails, in denen das Virus enthalten war, wurden sorgfältig maskiert als Geschäftskorrespondenz und trafen mehrere Tage, teils Wochen vorher ein.

Es gibt die Information darüber, dass Datum und Startzeit des Virus im Code verschlüsselt waren – 27. Juni 11:00 Uhr.

Am Vorabend des Tages der Verfassung (in der Ukraine ist heute ein Feiertag, A.d.Ü.) geschah die größte Cyberattacke auf Computersysteme von Finanzinstituten, Energieunternehmen, Massenmedien, Objekten der Transportinfrastruktur, Telekommunikationsnetze und andere große Organisationen in der Geschichte der Ukraine.

Auf den Rechner geratend, verschlüsselte das Erpresservirus alle Daten und forderte 300 Dollar in Bitcoins zu zahlen. Nach der Überweisung versprachen die Kriminellen, den Schlüssel für die Entschlüsselung zu schicken.

Von der Cyberattacke waren mehr als 100 Unternehmen in der gesamten Ukraine betroffen. Das erste war die Oshschadbank (Sparkasse), ihr folgten die UkrPotschta (Ukrainische Post), die Nowaja Potschta, UkrEnergo, UkrTelekom, das Ministerium für Infrastruktur, das Energieministerium, der 24. Kanal, Inter, der Erste Staatliche Kanal und viele andere.

Die Aussendung der E-Mails mit dem Virus fand an Firmenadressen statt, doch gab es auch Fälle der Ansteckung von privaten Computern.

Die Regierung meint, dass das Virus dafür gestartet wurde, um die Situation in der Ukraine zu destabilisieren, doch sagte Ministerpräsident Wladimir Groisman: „Die Attacke wurde abgewehrt und die Verbrecher aufgedeckt.“

Spezialisten für Cybersicherheit haben bereits Maßnahmen zur Stabilisierung der Situation ergriffen, versuchen herauszufinden, woher das Virus stammt und versuchen ebenfalls Unternehmen dabei zu helfen, die Folgen der Attacke zu beseitigen.

Es wird hervorgehoben, dass Computer mit dem Betriebssystem Windows 7 und darunter in Mitleidenschaft gezogen wurden. Computer, die mit Windows 10 und anderen Betriebssystemen arbeiten, haben nicht unter der Attacke gelitten.

In der Zone des besonderen Risikos

Den Worten des CEOs des Unternehmens SOC Prime, Andrej Beswerchij, nach hat das Virus nicht nur die Ukraine angegriffen, sondern auch andere Länder darunter die Niederlande, Polen und Frankreich.

Seinen Worten nach haben Spezialisten für Cybersicherheit bereits Indikatoren für die Attacke herausgefunden. In Verbindung damit wird erwartet, dass Microsoft ein kostenloses Updatepaket für Windows innerhalb der nächsten zwei Stunden herausgibt. Außerdem entdecken 13 Antivirusprogramme das Virus bereits und ihre Zahl steigt ständig.

Im gegenwärtigen Moment ist nicht zuverlässig bekannt, wie das Virus auf die Computersysteme gelangte. Doch auf diese Frage wird nach der Durchführung eines Reverse-Engineerings des Quellcodes der Schadsoftware eine eindeutige Antwort gegeben werden.

Bislang werden drei Ansteckungsszenarien in Betracht gezogen:

1. ein Link in einer E-Mail, der auf die Seite mit dem Download der Schad-Software führt
2. eine Ansteckung über die Systeme des elektronischen Dokumentenverkehrs (die ukrainische Cyberpolizei hält diese Variante über die [Updatefunktion der Buchhaltungssoftware M.E.Doc](#) für am Wahrscheinlichsten, A.d.Ü.)
3. ein Hack des Updatesystems von Windows, doch das liegt bisher auf der Ebene von Gerüchten

Andrej Beswerchij zufolge haben Spezialisten bisher keine Beweise, dass das Virus eine neue Modifikation von WannaCry ist. Bisher zeigt die Schadsoftware Anzeichen einer älteren Ransomware, die Petya heißt. Jedoch schließt Beswerchij nicht aus, dass das Virus Teile des Quellcodes von Petya und WannCry enthält.

Derweil meint der technische Direktor von Zillya!, Oleg Sytsch, dass das Virus dennoch eine neue Modifikation von WannaCry ist.

„Man kann es unterschiedlich benennen, beispielsweise schreiben sie auf der Seite der UkrPotschta, dass sie vom Trojaner Petya.A angegriffen wurden“, meint Sytsch. „Doch geht die Rede eher von WannaCry. Ungeachtet dessen, dass die neue Modifikation bedeutend verbessert wurde, gibt es offensichtliche Übereinstimmungen.“

Seinen Angaben nach fanden die ersten Ansteckungen per E-Mail statt.

Die Kriminellen sendeten Spam-Mails mit Arbeitsangeboten aus. Nach der Ansteckung des ersten Rechners drang der Trojaner, Verwundbarkeiten des Betriebssystem Windows ausnutzend, in lokale Netze ein und steckte alle anderen Computer des Netzes an.

Nach der Attacke von WannaCry im Mai hat Windows ein Update herausgebracht, das die Schwachstelle des Systems schloss, über das sich das Virus verbreitete. Bislang ist nicht gesichert bekannt, ob das neue Virus Systeme angriff, die nicht erneuert wurden, doch einigen Anzeichen nach kann man darauf schließen, dass das Virus eine neue Schwachstelle gefunden hat – die betroffenen Nutzer beteuern, dass ihr Windows vollständig up to date war. Wenigstens war der Patch für die WannaCry-Lücke installiert.

„Dabei kommt die Frage auf, warum das Virus so viele Personalcomputer ansteckte?“, sagt der technische Direktor von Zillya!. „Die Aufmerksamkeit verursacht auch die Tatsache, dass mehr als andere Unternehmen mit großen internen Netzen, die eine verzweigte Struktur haben, betroffen waren.“

Die Büros dieser Unternehmen sind physisch über das ganze Land verteilt, doch so organisiert, dass sie in einem einheitlichen Netzwerkraum arbeiten. In diesem Fall, wenn es an irgendeiner Stelle einen Einbruch gibt, das heißt ein Nutzer einen Trojaner bei sich startet, dann steckt der Trojaner alle Unterabteilungen unabhängig davon an, wo diese sich territorial befinden. Das Virus nutzt die logistische Struktur des lokalen Netzwerks. Daher haben vor allem große Unternehmen ein hohes Ansteckungsrisiko.

Hervorzuheben ist, dass das Trojanerprogramm nicht nur Arbeitscomputer ansteckt, sondern auch Server, die mit dem Betriebssystem Windows arbeiten und der Verlust von Informationen auf den Servern ist noch schmerzhafter.

Verhüten und Besiegen

Den Worten des Architekten des Sicherheitssystems des Unternehmens IT-Integrator, Alexej Schwatschki, nach nutzt das Virus die Windows-Schwachstelle unter der Bezeichnung [MS17-010](#) aus.

Spezialisten bestätigen, dass diese Schwachstelle seit März 2017 bekannt ist und dass Microsoft bereits seit Langem einen Sicherheitspatch herausgebracht hat, darunter auch für die bereits nicht mehr unterstützten

Windows Windows XP / Vista / 2003 / 2008.

„Wenn Sie eine dieser Versionen des Betriebssystems Windows nutzen, müssen sie unbedingt den Patch installieren, der unter der Adresse <http://www.catalog.update.microsoft.com/Search.aspx?q=4012598> zur Verfügung steht.

Für aktuelle lizenzierte Versionen des Betriebssystems Windows wird das Update automatisch installiert. Wenn es aus irgendeinem Grund nicht ausgeführt wird, dann kann die Anleitung zur Installation hier finden: <https://support.microsoft.com/de-de/help/4023262/how-to-verify-that-ms17-010-is-installed>

Wenn es den Verdacht gibt, dass Ihr Computer bereits infiziert ist, dann müssen unbedingt schnell wichtige Daten auf einen externen Datenträger kopiert werden, der danach unbedingt ausgeschaltet werden muss.“

Denjenigen, die bisher nicht infiziert wurden, empfiehlt Oleg Sytsch per Firewall die Ports 135 und 139 zu sperren. Auf diese Weise können Nutzer keine Verzeichnisse und Datenträger im Netz öffnen, doch alle anderen Transportprotokolle bleiben zugänglich. Sowohl Internet, als auch Messenger und E-Mail funktionieren weiter. Der Dateiaustausch wird nicht funktionieren, doch damit ist die Ausbreitung des Trojaners blockiert.

Denjenigen, die bereits betroffen sind, empfiehlt Oleg Sytsch alle Festplatten von den Arbeitsplattformen zu entfernen und sie einzulagern. Anstelle dessen sollten neue Festplatten mit frischen Betriebssystemen installiert werden.

„Die Wahrscheinlichkeit, dass die Daten dennoch entschlüsselt werden können, existiert“, sagt der technische Direktor von Zillya!.

Bleibt zu erwähnen, dass nach der Attacke von Petya im April 2016 kostenlose Dechiffrierer der verschlüsselten Dateien auftauchten. Diese wurden von mehreren Spezialisten aus unterschiedlichen Ländern erstellt, nachdem der Code des Verschlüsselungserpressers geknackt wurde.

Übrigens, damit man nachher nicht auf das Auftauchen eines Entschlüsselprogramms hoffen muss, ist es besser, die Basisregeln für die Arbeit mit E-Mail und verschickten Dateien zu lernen. An diese Regeln wurde im Unternehmen Kyivstar erinnert, das von der Attacke nicht betroffen war:

1. Öffnen Sie keine Links auf Webseiten, die sie in verdächtigen E-Mails oder SMS erhalten haben. In keinem Fall Programme starten, die auf derartige Weise heruntergeladen oder installiert werden sollen. Kriminelle können den Empfänger mit Gewinnspielen, der Nutzung von Logotypen bekannter Unternehmen, dem Aufruf zu unverzüglichen Handlungen und anderen Methoden der sozialen Manipulation hereinlegen.
2. Überprüfen Sie aufmerksam die Adresse von Webseiten oder die Absenderadresse von E-Mails. Besonders aufmerksam muss man in dem Fall sein, wenn Sie aufgefordert werden Login und Passwort einzugeben.
3. Öffnen Sie keine E-Mail-Anhänge, die von unbekannten Absendern stammen. Wenn es den kleinsten Verdacht bezüglich des Inhalts der E-Mail gibt, überprüfen Sie den Anhang unbedingt mit einem Antivirusprogramm. Im Fall des Entdeckens eines Virus löschen Sie die E-Mail unbedingt und leeren den „Papierkorb“.
4. Installieren Sie auf Computern und mobilen Geräten keine Programme aus inoffiziellen Quellen. Die Programme können versteckte schädliche Funktionen enthalten, die von Schutzsystemen nicht entdeckt werden.
5. Gehen Sie mit Bedacht mit ihren Passwörtern um, nutzen Sie schwierige Passwörter, nutzen Sie nicht ein und dasselbe Passwort bei verschiedenen Systemen, sowohl bei Unternehmensadressen als auch bei persönlichen Adressen. Setzen Sie unbedingt ein Passwort für die Blockierung Ihres mobilen Geräts.

Und für Anhänger radikaler Lösungen dient das Beispiel der PrivatBank. Sie wurde 2013 zum größten Unternehmen in der Welt, welches das Betriebssystem Linux nutzt.

„Für unsere Softwarekomplexe und -systeme existieren zum heutigen Tag keine Bedrohungen durch Hacker, in

vielen dank der Konfiguration der Systeme und der Arbeit der Abteilung für elektronische Sicherheit“, teilte heute der Pressedienst der PrivatBank mit.

27. Juni 2017 // **Wsewolod Nekkassow, Alina Poljakowa**

Quelle: [Ekonomitscheskaja Prawda](#)

Übersetzer: **Andreas Stein** — Wörter: 1463

Namensnennung-Keine kommerzielle Nutzung-Weitergabe unter gleichen Bedingungen 3.0 Deutschland Sie dürfen:

- das Werk vervielfältigen, verbreiten und öffentlich zugänglich machen
- Bearbeitungen des Werkes anfertigen

Zu den folgenden Bedingungen:

Namensnennung. Sie müssen den Namen des Autors/Rechteinhabers in der von ihm festgelegten Weise nennen (wodurch aber nicht der Eindruck entstehen darf, Sie oder die Nutzung des Werkes durch Sie würden entlohnt).

Keine kommerzielle Nutzung. Dieses Werk darf nicht für kommerzielle Zwecke verwendet werden.

Weitergabe unter gleichen Bedingungen. Wenn Sie dieses Werk bearbeiten oder in anderer Weise umgestalten, verändern oder als Grundlage für ein anderes Werk verwenden, dürfen Sie das neu entstandene Werk nur unter Verwendung von Lizenzbedingungen weitergeben, die mit denen dieses Lizenzvertrages identisch oder vergleichbar sind.

- Im Falle einer Verbreitung müssen Sie anderen die Lizenzbedingungen, unter welche dieses Werk fällt, mitteilen. Am Einfachsten ist es, einen Link auf diese Seite einzubinden.
- Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.
- Diese Lizenz lässt die Urheberpersönlichkeitsrechte unberührt.

Haftungsausschluss

Die Commons Deed ist kein Lizenzvertrag. Sie ist lediglich ein Referenztext, der den zugrundeliegenden Lizenzvertrag übersichtlich und in allgemeinverständlicher Sprache wiedergibt. Die Deed selbst entfaltet keine juristische Wirkung und erscheint im eigentlichen Lizenzvertrag nicht.

Creative Commons ist keine Rechtsanwaltsgesellschaft und leistet keine Rechtsberatung. Die Weitergabe und Verlinkung des Commons Deeds führt zu keinem Mandatsverhältnis.

Die gesetzlichen Schranken des Urheberrechts bleiben hiervon unberührt.

Die Commons Deed ist eine Zusammenfassung des Lizenzvertrags in allgemeinverständlicher Sprache.