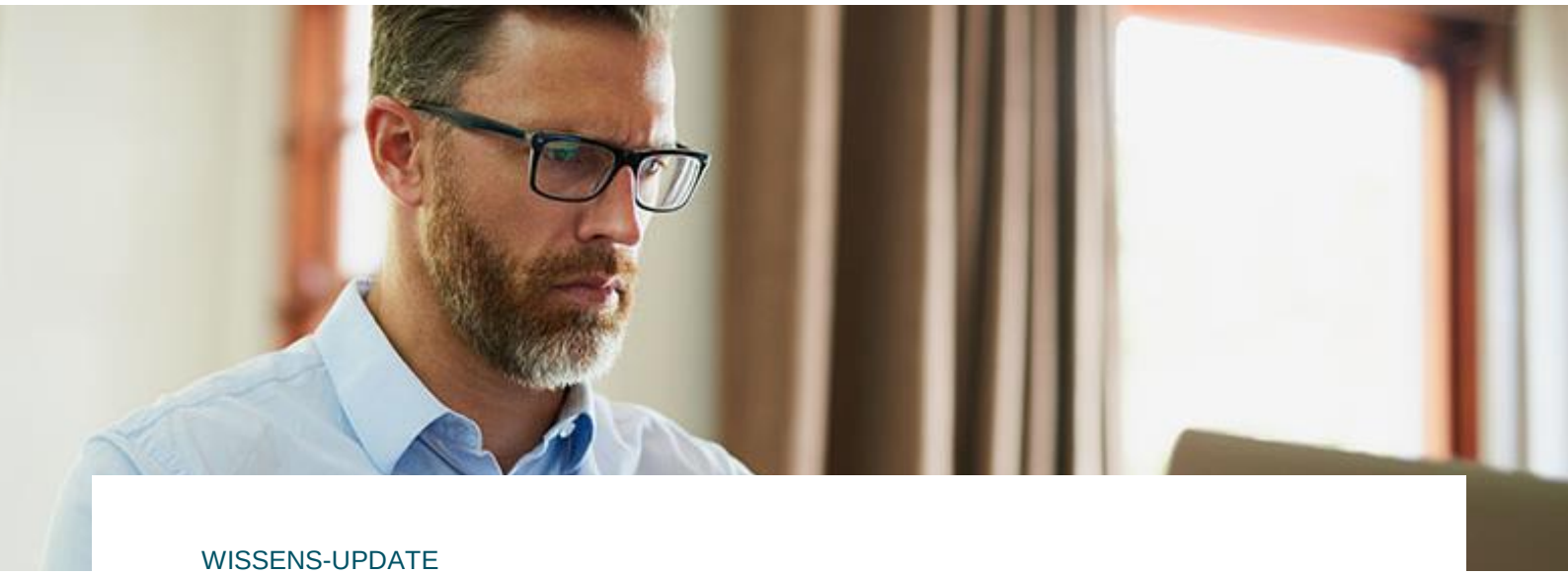
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WISSENS-UPDATE

Die 3 wichtigsten Malware Trends 2021

Steinhausen, 05. Januar 2021

Fast unbemerkt von der Öffentlichkeit fand im Herbst 2020 eine von staatlichen und privaten US-Organisationen koordinierte Cyber-Operation gegen Trickbot statt . Hat diese mit einer vorbildlichen Public-Private Partnerschaft und professionell durchgeführte US Cyber-Operation Trickbot endgültig den Garaus gemacht und mit welchen Malware Trends müssen wir 2021 rechnen?

Generell werden wir im cyber-kriminellen Umfeld auch 2021 das anhaltende Muster mit Phishing und dem gezielten Einsatz von Ransomware auf zivile Unternehmen beobachten. Dabei werden noch besser auf die einzelnen Unternehmen ausgerichtete Phishing-E-Mails zum Einsatz kommen. Die Gründe dafür liegen auf der Hand: Cyber-Kriminelle können einerseits mit disruptiver Malware weitaus mehr und schneller Geld erpressen als mit herkömmlich gestohlenen Informationsdaten. Andererseits haben die durch die Covid-19-Pandemie verstärkten Homeoffice-Aktivitäten die damit verbundenen Remote-Zugriffe auf Unternehmensinfrastrukturen den Cyber-Kriminelle eine immens grosse Anzahl an neuen möglichen Angriffszielen gegeben. Damit einher geht vermutlich auch eine grössere Anzahl von Online Scams und Malicious Domains.

Für 2021 sehen wir nachfolgende 3 Haupttrends:

Trend 1: Post-Covid-19- Massnahmen gegen «FakeUpdates» und «Zerologon»
Seit Beginn der Covid-19-Pandemie sind sogenannte Kollaborations-Plattformen nicht mehr wegzudenken. Viele Unternehmen, Behörden und Bildungsinstitute setzen dabei auf das «Microsoft Teams»-Produkt. Das Programm ist eine Art virtueller Arbeitsplatz in «Microsoft 365», mithilfe dessen die Benutzer an verschiedenen Orten in einem virtuellen Team zeitgleich an Dokumenten

arbeiten können. Zusätzlich werden dabei auch Sprach- und Chatfunktionen für das gemeinsame Arbeiten zur Verfügung gestellt. Das Programm fokussiert vor allem auf eine moderne und dynamische Arbeits- und Kommunikationsweise für Unternehmen und Schulen, an welche vor allem die Young Professionals gewöhnt sind.

Auch Cyber-Kriminelle haben in der verbreiteten Anwendung von «Microsoft Teams» Potenzial erkannt – für neue Angriffe: «FakeUpdates» ist eine Kampagne, mit welcher Anwender irregeführt werden, um vermeintliche Updates für «Microsoft Teams» herunterzuladen. In Wirklichkeit wird aber Payload heruntergeladen, um Malware in den Netzwerken der attackierten Organisationen zu verbreiten. Um die Benutzer zum Herunterladen der gefälschten Updates zu bewegen, verwenden die Cyber-Kriminellen seriös erscheinende Werbeanzeigen in verschiedenen Suchmaschinen (z.B. Google Ads), um potenzielle Opfer anzulocken. Klickt das ausgesuchte Opfer auf den Link, wird die initiale Nutzlast heruntergeladen, welche auf dem Zielgerät ein PowerShell-Skript ausführt und die Hintertür darstellt. Um keinen Verdacht zu erwecken, wird dabei eine legitime Version von «Microsoft Teams» heruntergeladen. In der Quintessenz sind infizierte Werbebanner verglichen mit dem aufwendigen Hacken von Webseiten lukrativer für Cyber-Kriminelle: Durch das rege Klicken auf den Link wird dieser zu einem der Top-Suchergebnissen bei verschiedenen Suchvorgängen, denn der PageRank-Algorithmus bewertet die verlinkte Seite im Zuge der Web-Indexierung als populär und relevant – die Link Popularity und schliesslich der PageRank-Wert steigen, was den Cyber-Kriminellen wiederum in die Karten spielt.

Vor allem durch die Kombination dieser «FakeUpdates» mit der vom Secura-Team veröffentlichten «Microsoft Zerologon»-Sicherheitslücke («Netlogon»-EoP-Schwachstelle CVE-2020-1472) sehen wir für 2021 eine erhöhte Gefahr für lokale Unternehmens- und Behördennetzwerke. «Zerologon» bezeichnet einen Fehler im Protokoll «Netlogon», das wiederum von Windows-Systemen benutzt wird, um sich bei einem Windows-Server zu authentifizieren, der als Domain Controller agiert. Angreifer sind unter Umständen in der Lage, die Kontrolle über den Domain Controller zu übernehmen. Bereits haben verschiedene Cyber-Sicherheitsunternehmen davor gewarnt, dass mehrere cyber-kriminelle Gruppierungen den öffentlichen Exploit in ihr Angriffsarsenal übernommen haben.

Trend 2: Neue Trickbot-Varianten?

Nach dem koordinierten Vorgehen des U.S. Cyber Commands zusammen mit Microsoft und diversen US-Hosting Providern sind die Trickbot-Aktivitäten mit den involvierten Schadprogrammen Emotet und Ryuk anfangs November 2020 um bis zu 90% zurückgegangen.

Leider zeigen erste Analysen auf, dass es den Trickbot-Betreibern während und im direkten Nachgang zu den durchgeführten aktiven Cyber-Operationen der US-Behörden zusammen mit den involvierten US-Unternehmen gelungen ist, schnelle Gegenmassnahmen einzuleiten. Einerseits konnten die Trickbot-Betreiber teilweise eine Persistenz auf den infizierten Infrastrukturen erreichen, zum Beispiel durch den Einsatz von CobaltStrike. Andererseits wurden rasche Modifikationen an den Konfigurationsdateien von Trickbot vorgenommen, was eine weitere Entdeckung durch die Ermittler temporär erschwerte.

Für die erste Hälfte 2021 rechnen wir mit einer zunehmenden Zahl von initialen Angriffen basierend auf dem BazarLoader – dies aufgrund der Source Code-Ähnlichkeit und der teilweise gemeinsam genutzten Infrastrukturen. Spätestens ab der zweiten Jahreshälfte ist wieder verstärkt mit Trickbot zu rechnen. Wir gehen dabei von einer grösseren Varietät der Trickbot-Konfigurationsdateien auf verschiedenen Infrastrukturen aus. Zudem kann mit einer viel höheren Adaptionsdynamik gerechnet

werden. Damit wollen die Verantwortlichen verhindern, dass sich ein erneuter Kahlschlag ihrer Trickbot-Infrastruktur wie im Oktober 2020 wiederholt.

Trend 3: NTP, die kritische Komponente
Die sogenannten Infrastrukturprotokolle sind seit langem ein beliebtes Ziel von Cyber-Kriminellen. Im 2020 sind auffällig viele neue Managementlösungen für die zentrale Verwaltung von DNS, DHCP, aber auch IP-Ranges aufgetaucht. Dies liegt womöglich daran, dass viele Unternehmen durch den ganzen Covid-19-Remotezugriff bessere Tool Sets benötigt haben bzw. haben werden, mit welchem die verantwortlichen Administratoren diese Protokolle domänen- und netzwerkübergreifend verwalten, konfigurieren und sichern können.

In diesem Zusammenhang war es 2020 auch interessant zu sehen, dass vor allem die Unterstützung für die Verwendung von sicherem DNS zugenommen hat – dies vor allem, um MitM-Attacks (Man-in-the-Middle) sowie das Spoofing von internetbasierten Diensten (DNS Cache Poisoning) besser verhindern zu können.

Aus unserer Sicht könnte 2021 das NTP (Network Time Protocol) vermehrt in den Fokus von Cyber-Kriminellen geraten. Immerhin hilft dieses Protokoll, alle zeitabhängigen Aufgaben innerhalb einer Organisation oder Unternehmens zu steuern. Wenn das Timing nicht stimmt, können viele grundlegenden Dienstleistungen, angefangen von der Lizenzierung von Servern bis hin zu «batch-based» Aufgaben fehlschlagen. Dies kommt einem eigentlichen Denial-of-Service-Angriff (DoS) ziemlich nahe. Schlüsselinfrastrukturen, sei es im Internet und / oder innerhalb der Backend-Prozesse eines Unternehmens können dadurch jedenfalls stark beeinträchtigt werden.

Wir erwarten daher, dass 2021 neue Schwachstellen, Exploits und Malwares, welche auf Zeitserver und andere ältere Protokolldienste abzielen, Unternehmen oder Behördenorganisationen stören können. In Kombination mit dem Einsatz von Ransomware können solche erfolgreichen Exploits die Wiederherstellung zudem erschweren und dadurch verzögern.

Verlässlicher und umfassender Schutz ist gefragt
Damit Ihre Verwaltungseinheit auch zukünftig von den neuen, zunehmend professionelleren Cyber-Bedrohungen optimal geschützt und Ihre sensiblen Daten sicher sind, braucht es einen umfassenden «Cyber Defence in Depth»-Ansatz. Auch empfehlen wir Software-Entwicklern die vorgängige sicherheitstechnische Überprüfung von eingesetzten Software-Libaries. Die CyOne Security kann hier als Review-Partner eine kompetente Überprüfung durchführen.

Die CyOne Security ist Ihr vertrauensvoller Partner
Setzen Sie dafür auf die langjährige Erfahrung und die 360°-Sicherheitskompetenz der CyOne Security. Als rein schweizerisches Unternehmen bieten wir den kundenspezifischen Risiken angepasste, umfassende Sicherheitskonzepte und -lösungen auf höchstem Niveau für Product Security, System Security sowie Operational Security an.

Beginnen Sie heute, Ihre Organisation und somit die Schweiz vor Cyber-Risiken zu schützen.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Experten Ihre aktuellen und zukünftigen Cyber-Sicherheitsbedürfnisse und entsprechende Sicherheitslösungen.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.