Cyberdefence 24

aut. Szymon Palczewski 11.03.2021

HAKERZY RZUCILI SIĘ NA LUKI W MICROSOFT EXCHANGE

Hakerzy, należący do ponad 10 różnych grup APT, wykorzystali luki w oprogramowaniu Microsoft Exchange do prowadzenia kampanii nie tylko w Stanach Zjednoczonych, lecz na całym świecie, w tym w regionie Europy Wschodniej. Działania miały głównie charakter cyberszpiegostwa, a ich celem były instytucje państwowe oraz firmy prywatne. Które grupy wykazywały największą aktywność?

Dokładnie 2 marca br. Microsoft poinformował o wykryciu „wielu exploitów zero-day", które były używane do ataków na oprogramowanie Microsoft Exchange w ramach ukierunkowanych operacji hakerskich. Podczas wrogich działań wykorzystano luki w celu uzyskania trwałego dostępu do serwerów, co miało ułatwić zewnętrznemu aktorowi wgląd do kont e-mail ofiar oraz umożliwić zainstalowanie na ich urządzeniach złośliwego oprogramowania.

Jak informowaliśmy na naszym portalu, zespół Microsoft Threat Intelligence Center (MSTIC) przypisał kampanię grupie „Hafnium", która jest podmiotem sponsorowanym przez państwo. Specjaliści wskazali, że hakerzy są powiązani z Chinami, lecz działają poza granicami Państwa Środka, o czym świadczą zebrane podczas analizy dowody.

W ramach operacji wykorzystano konkretnie cztery luki w oprogramowaniu Microsoft Exchange: CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 oraz CVE-2021-27065. Amerykański koncern w reakcji na wrogie działania wydał aktualizację, która miała zlikwidować wskazane wyżej podatności.

Czytaj też: Hakerzy powiązani z Chinami wykorzystali podatności w produkcie Microsoftu

Początkowo wskazywano, że poszkodowane są przede wszystkim firmy, organizacje i instytucje ze Stanów Zjednoczonych. Jak podano, włamano się do 30 tys. podmiotów w USA, co skłoniło administrację Joe Bidena do opracowania planów powołania specjalnego zespołu zadaniowego, który ma uporać się z sytuacją związaną z kampanią prowadzoną przez chińskich hakerów. Miałby nazywać się „Unified Coordination Group" i składać z przedstawicieli FBI, CISA oraz innych organizacji.

Czytaj też: USA: specjalny zespół zajmie się „chińskim hakiem dekady"

Z czasem okazało się jednak, że podczas kampanii, w ramach której wykorzystano podatności w Microsoft Exchange, hakerzy włamali się nie tylko do amerykańskich, ale również 250 tys. innych podmiotów z całego świata. Przewiduje się jednak, że liczby te ulegną zwiększeniu.

Jednym z celów ataku był Europejski Urząd Nadzoru Bankowego (ang. European Banking Authority – EBA). Jak informowaliśmy na naszym portalu, do czasu opanowania sytuacji agencja zdecydowała się

na wyłączenie systemów poczty elektronicznej.

Czytaj też: Hakerzy atakują unijną instytucję

Najnowsza analiza przeprowadzona przez specjalistów ESET wykazała, że luki w produkcie Microsoftu były wykorzystywane nie tylko przez jedną grupę hakerską (Hafnium), lecz przez „ponad 10 różnych podmiotów APT". Wśród nich eksperci wyszczególnili m.in.:

- Tick – grupa, działająca od 2008 roku, której celem są organizacje z Japonii, Korei Południowej, Rosji i Singapuru. Jej głównym celem jest kradzież własności intelektualnej i informacji niejawnych. Najczęściej wykorzystywanym narzędziem hakerskim jest wirus Daserf, xxmm i Datper, a także Lilith (RAT).
- Lucky Mouse – znana również jako APT27 lub Emissary Panda – to grupa cyberszpiegowska, o której wiadomo, że w 2016 roku włamała się do wielu sieci rządowych w Azji Środkowej i na Bliskim Wschodzie, a także do organizacji międzynarodowych, w tym Międzynarodowej Organizacji Lotnictwa Cywilnego. Bardzo sprawnie posługuje się złośliwym oprogramowaniem HyperBro i SysUpdate.
- Calypso – podmiot APT specjalizujący się w cyberszpiegostwie, którego podstawowym celem są instytucje rządowe w regionie Azji Środkowej, Ameryce Południowej i na Bliskim Wschodzie. Słynie z operacji z wykorzystaniem PlugX RAT.
- Websiic – ugrupowanie hakerskie, którego ofiarami są firmy prywatne z takich sektorów jak IT oraz telekomunikacja, działające w Azji oraz organy rządowe w Europie Wschodniej.
- Winnti Group – aktor APT aktywny od co najmniej 2012 roku, który jest odpowiedzialny za liczne cyberataki na podmioty oprogramowania przemysłowego oraz branży gier wideo. Zakres wrogich działań hakerów grupy obejmuje również sektor ochrony zdrowia i edukacji.
- Tonto Team – jego hakerzy prowadzą wrogie operacje od co najmniej 2009 roku, uderzając przede wszystkim w cele rządowe i instytucje państwowe Rosji, Japonii oraz Mongolii. Grupa sprawnie posługuje się narzędziem Bisonal RAT.
- Mikroceen – znana również jako Vicious Panda – to aktor, który działa od co najmniej 2017 roku, a jego ofiarami są przede wszystkim podmioty rządowe i firmy telekomunikacyjne z regionu Azji Środkowej, Rosji oraz Mongolii. Podczas cyberataków hakerzy używają charakterystycznego wirusa, którego określenie nawiązuje do nazwy grupy – Mikroceen RAT.
- DLTMiner – jest to podmiot APT, który różni się od pozostałych tym, że jego główną specjalizacją jest wydobywanie kryptowalut.

ESET w swoim raporcie podkreślił, że część z wymienionych wyżej grup hakerskich (np. LuckyMouse, Calypso i Winnti Group) prowadziły wrogie operacje zanim amerykański koncern wydał aktualizację do swojego produktu. Z kolei m.in. Tonto Team i Mikroceen realizowały swoją kampanię już po udostępnieniu łatek przez Microsofta.

Luki w Microsoft Exchange posłużyły hakerom do licznych operacji w różnych częściach świata. Poza znanymi już ofiarami, takimi jak Europejski Urząd Nadzoru Bankowego czy 30 tys. amerykańskich podmiotów z wielu branż, specjaliści ESET wskazują na włamania na serwery poczty elektronicznej organizacji i instytucji rządowych na Bliskim Wschodzie, w Ameryce Południowej, Afryce, Azji oraz Europie. Eksperci podali także przykład dwóch firm (zaopatrzeniowej oraz konsultingowej) ze wschodniej części Starego Kontynentu, lecz nie wymienili konkretnych nazw poszkodowanych podmiotów.

Skalę zagrożenia pokazują dane udostępnione przez niemieckie Federalne Biuro Bezpieczeństwa

Informacji (...). Zgodnie z opublikowanymi statystykami podatności w Microsoft Exchange naraziły łącznie około 60 000 systemów komputerowych w kraju.

Jak podkreślił Arne Schönbohm, szef BSI, ponad połowa luk została usunięta po tym, jak Biuro wydało specjalne ostrzeżenie dotyczące nieprawidłowości występujących w produkcie Microsoftu. Jednak pomimo tego, około 25 000 systemów nadal wymaga wdrożenia poprawek bezpieczeństwa - donosi Agencja Reutera.

> *Ostrzeżenie zadziałało. W Niemczech wiele serwerów Exchange zostało zabezpieczonych poprzez pobranie poprawek. Każdy wrażliwy system to o jeden za dużo i może prowadzić do szkód.*
>
> Arne Schönbohm, szef Federalnego Biura Bezpieczeństwa Informacji

BSI potwierdziło, że w Niemczech doszło do włamania do dwóch podmiotów federalnych, dzięki wykorzystaniu luk w Microsoft Exchange. Służby nie podają jednak ani ich nazwy ani szerszych szczegółów na temat działań hakerów. Biuro zadeklarowało jedynie, że pozostaje w kontakcie ze wszystkimi zespołami reagowania na incydenty komputerowe (CERT) w Europie oraz w innych regionach świata, a zwłaszcza z amerykańską Agencją ds. Cyberbezpieczeństwa i Infrastruktury (CISA) oraz koncernem Microsoft.

Czytaj też: Hack dekady w wersji chińskiej. Biały Dom bada skutki wykrytych podatności