Akamai i Advatech dla sektora usług finansowych

Rozwiązania Akamai:

- Chronią bankowe strony transakcyjne przed atakami typu DDoS czy Credential Stuffing
- Zabezpieczają infrastrukturę DNS
- Mitygują największe ataki DDoS na infrastrukturę firmową
- Zapewniają integralność strony bankowej
- Pozwalają zarządzić ruchem botów
- Sprawiają, że strony i aplikacje działają szybciej

Dlaczego teraz?

- Wzrost aktywności grup przestępczych w internecie
- Wzrost wolumenu i złożoności ataków DDoS
- Nowe wektory ataków
- Historycznie duża aktywność botnetów

Dlaczego Akamai?

Zaufało nam:

- 10 z 10 największych banków europejskich
- Ponad 700 firm świadczących usługi finansowe na całym świecie
- Ponad 400 banków na całym świecie
- Wszystkie 25 największych banków w USA
- Akamai jest w rejestrze dostawców usług dla Visa i MasterCard
- Zgodność z PCI DSS
- Web Application Firewall wyróżniony przez Garnera i Forrestera
- 20 scrubbing centers, gdzie mitygowane są ataki Ddos
- 6 globalnych centrów SOC , w tym jeden w Polsce
- Biuro w Krakowie
- 7500+ pracowników na świecie, z czego 800+ w Polsce
- 20 lat doświadczeń i obecność na NASDAQ

Zapraszamy do kontaktu

Hubert Ortyl | hortyl@advatech.pl

Advatech jest jednym z czołowych integratorów na polskim rynku z ponad 20-letnim doświadczeniem, zaufanym dostawcą infrastruktury, oprogramowania, rozwiązań wirtualizacyjnych i bezpieczeństwa m.in. takich marek jak: Akamai, IBM, Oracle, Dell EMC, Hitachi Vantara, HPE, HP Inc, VMware, Veritas, Veeam, Ivanti, Barracuda, Commvault, Microsoft, Red Hat, NetApp, Brocade, Symantec i Fortinet.

Firma posiada szerokie kompetencje potwierdzone certyfikacjami pozwalające na kompleksową obsługę Klientów, od Proof of Concept, przez wdrożenia po utrzymanie serwisów.

Advatech od wielu lat znajduje się w czołówce najdynamiczniej rozwijających się firm IT na rynku środkowoeuropejskim i regularnie bierze udział w rankingach m.in.: Computerworld TOP200, ITwiz Best 100.

Advatech posiada 4 oddziały w Polsce: we Wrocławiu, Warszawie, Poznaniu i Katowicach.

Gra się nie skończyła

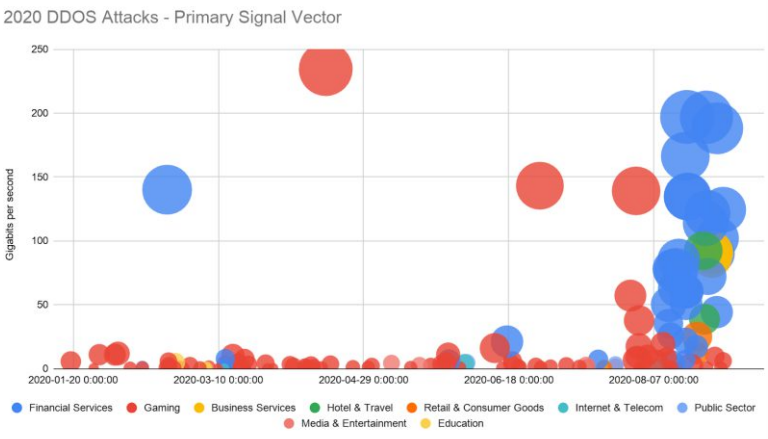
Nowa fala cyber ataków: Ransomware, Extortion, DDos Threats

Jeśli chodzi o ataki DDoS to można powiedzieć, że rok 2020 był raczej „nudny". Podekscytowanie związane z rekordowymi atakami (1.44 Tbps czy +800 Mpps), obserwowanymi wczesnym latem, minęło i nie widzieliśmy wielu interesujących incydentów.

Sytuacja zmieniła się gwałtownie na początku sierpnia 2020, gdy fala listów z żądaniami okupu i związanymi z nimi atakami typu DDoS, została wymierzona w firmy z wielu branż, w tym najbardziej intensywnie w instytucje finansowe. Grupy powiązane z tą kampanią to chyba wszystkim już dobrze znane Fancy Bear, Cosy Bear czy Armanda Collective.

Ransom DoS (RDoS) nie jest nowością ani dla Akamai, ani dla naszych klientów. Zajmujemy się tym problemem i tymi grupami tak długo, jak one istnieją. Ataki DDos są wpisane w ryzyko biznesowe: były, są i będą. Kampanię tą wyróżnia jednak kilka charakterystycznych elementów: jest rozproszona, ataków jest dużo i są większe, nie są typowe, składają się z dużej liczby wektorów, trwają długo.

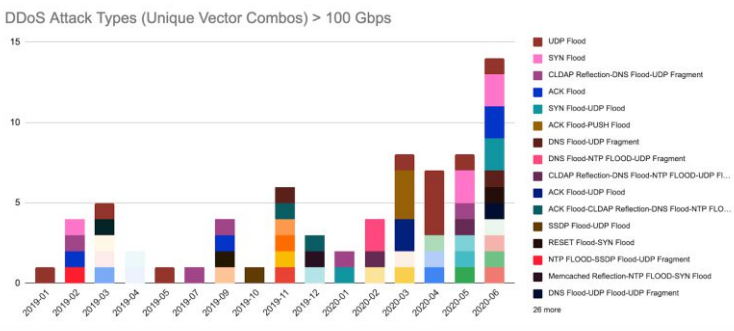
Z obserwacji z ostatnich kilku tygodni wynika, że kampania ta trwa w wielu krajach. Atakowane są różne branże: głównie instytucje finansowe. branża e-commerce. Gaming czy Hotel&Travel.



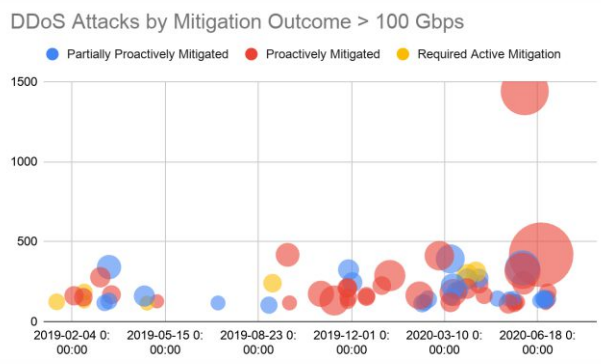
Co jeszcze wyróżnia tą kampanię i ataki z nią związane? Na pewno liczba ataków i ich wielkość (zarówno w wartościach BPS czy PPS). Co więcej, wiele kampanii wymuszających DDoS zaczyna się od listu z groźbą i nigdy nie wykracza poza ten punkt. W przypadku takich kampanii, często dochodzi do „próbnych" ataków, nawet o wielkości 200 Gbps. W ten sposób przestępcy udowadniają celowi, że mogą znacząco utrudnić mu życie. Możemy jednak założyć, że pomimo najlepszych starań atakujących wiele e-maili z wymuszeniami trafia do filtrów spamowych lub do śmieci, bez dalszych przykrych konsekwencji.

Prócz wielkości i częstotliwości ataków, faktem który przykuwa również uwagę jest ich złożoność. Ataki, które obserwujemy składają się często z wielu różnych wektorów. Jako przykład mogę podać atak z czerwca 2020 na jeden z europejskich banków - użyto 9 różnych wektorów ataku, pochodzących z osobnych narzędzi. Jest to rzadkością, ponieważ większość ataków DDoS obserwowanych przez Akamai korzysta z 1-3 różnych wektorów atakujących.

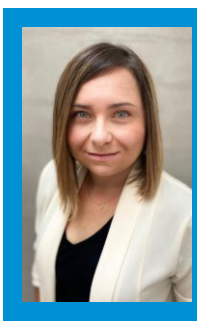
Co również istotne, w chwili obecnej przestępcy są dużo mądrzejsi niż kiedyś - prowadzą ataki w skoordynowany sposób, przez określoną długość czasu, nie są to już minuty czy sekundy, ale nawet godziny – wspomniany już atak DDoS utrzymywał poziom ruchu na poziomie około 1 Tbps i 200 milionów pakietów na sekundę przez około godzinę. W ten sposób atakujący celują w ważne wydarzenia, w momenty, które są istotne dla danego podmiotu.



Zwróciłabym uwagę na jeden bardzo ciekawy fakt - ponad 90% tych ataków może być premitygowana, tzn. mitygowana w 0 sekund za pomocą automatycznych kontroli i reguł. Same ataki nie są nowe, używają znanych wektorów i można tak skonfigurować swoje zabezpieczenia, aby były one w stanie ochronić organizację przed tego typu groźbami. Niestety, wiele organizacji nie ma odpowiednich zabezpieczeń lub z różnych powodów ich nie włączyło. Wiele z nich musiało podjąć działania awaryjne, w trybie tzw. Emergency Integration w czym pomógł im min. dedykowany do tego serwis Akamai Anti DDoS Prolexic oraz nasz SOCC. Jako ciekawostkę podam, że jeden z pięciu globalnych SOCCów Akamai znajduje się w Polsce, w Krakowie i działa w trybie 24/7.



Dzięki utrzymywaniu 30% dziennego ruchu w Internecie, Akamai Technologies posiada unikalną wiedzę odnośnie najnowszych zagrożeń, pochodzenia i typów najbardziej wyrafinowanych metod ataków hackerskich. Jest ona jest wykorzystywana do aktualizacji naszej bazy wiedzy, a co za tym idzie silnika wszystkich rozwiązań security na platformie Akamai. Aktualnie nasz platforma Prolexic sklada się z 20 scrubbing centers, ma pojemność ponad 8Tbps, i jak udowodniliśmy, jesteśmy w stanie odeprzeć największe ataki przekraczające 1 Tbps.



Magdalena Opala - Wróbel
Major Account Executive - Akamai Technologies Poland

Od ponad 13 lat jestem związana z branżą IT. Praca w Akamai Technologies, jednej z największych firm na świecie, która zajmuje się przyspieszaniem pracy w internecie, ochroną aplikacji webowych oraz bezpieczeństwem usług w chmurze, to jedno z najciekawszych doświadczeń zawodowych w moim życiu. Odpowiadam za rozwój rynku i rozwijanie relacji biznesowych z największymi firmami z sektora finansowego, publicznego, e-commerce, czy branży turystycznej w Polsce oraz w Europie Środkowo Wschodniej.