STUDIU Accenture: Hackerii sponsorizați de state și grupările ransomware își diversifică tacticile pentru a provoca mai multe pagube

Raportul Cyber Threatscape 2020 al Accenture dezvăluie amenințările prolifice care influențează peisajul cibernetic

București: 29 octombrie 2020 - Unii dintre cei mai pricepuți hackeri sponsorizați de state și de grupări cunoscute ransomware apelează la un arsenal de noi instrumente open-source pentru a exploata în mod activ sistemele de email ale corporațiilor, iar prin intermediul șantajului online intimidează victimele pentru a plăti răscumpărări, conform raportului Cyber Threatscape din 2020 de la Accenture (NYSE: ACN).

Valorificând capacitățile CTI (Cyber Threat Intelligence) ale Accenture, raportul produs anual de companie examinează tacticile, tehnicile și procedurile folosite de unii dintre cei mai sofisticați adversari cibernetici și explorează modul în care incidentele cibernetice ar putea evolua în anul următor. La raport au contribuit cercetători de la Context Information Security și Deja vu Security, companii pe care Accenture le-a achiziționat în martie 2020, respectiv iunie 2019. Pe lângă aceste achiziții, Accenture a mai preluat în acest an diferite companii, inclusiv Symantec's Cyber Security Services business și Revolutionary Security, demonstrând astfel angajamentul continuu al companiei de a-și extinde serviciile de securitate cibernetică pentru clienții săi.

Cercetătorii Accenture au descoperit numeroase campanii de phishing și amenințări pentru dispozitivele mobile, care profită de îngrijorarea publicului și confuzia cu privire la COVID-19 și utilizează pandemia ca momeală. Printre grupările detectate de specialiștii Accenture se numără: Lucifershark, Snipefish, Rohu sau Pond Loach.

„Deoarece COVID-19 a schimbat radical modul în care lucrăm și trăim, am văzut o gamă largă de adversari cibernetici schimbându-și tactica pentru a profita de noi vulnerabilități", a spus Josh Ray, care conduce divizia de apărare cibernetică a Accenture Security la nivel global. „Cea mai importantă informație din studiul nostru este că organizațiile ar trebui să se aștepte ca infractorii cibernetici să devină mai curajoși pe măsură ce potențialele oportunități și câștiguri din aceste campanii cresc. Într-un aceste condiții, organizațiile trebuie să dubleze punerea în aplicare a controalelor prin utilizarea informațiilor privind amenințările cibernetice pentru a înțelege și a elimina cele mai complexe amenințări."

Adversarii sofisticați își maschează identitățile cu instrumente off-the-shelf

Pe parcursul anului 2020, analiștii CTI ai Accenture au observat grupurile infracționale sponsorizate de state și grupări criminale organizate folosind o combinație de instrumente off-the-shelf – inclusiv instrumente de "living off the land", infrastructură de găzduire partajată și cod de exploatare dezvoltat public – și instrumente de testare a penetrării open source la o scară fără precedent pentru a efectua atacuri cibernetice și a-și ascunde urmele.

De exemplu, Accenture urmărește tiparele și activitățile unui grup de hackeri din Iran, denumit SOURFACE (cunoscut și sub numele de Chafer sau Remix Kitten). Activ din cel puțin 2014, grupul este cunoscut pentru atacurile cibernetice asupra industriilor de petrol și gaze, comunicații, transporturi dar și altele din SUA, Israel, Europa, Arabia Saudită, Australia și alte regiuni. Analiștii Accenture CTI au observat SOURFACE folosind funcții Windows legitime și instrumente disponibile în mod gratuit, cum ar fi Mimikatz, pentru dumping-ul de credențiale. Această tehnică este utilizată pentru a fura acreditările de autentificare ale utilizatorilor, cum ar fi numele de utilizator și parolele, pentru a permite atacatorilor să își extindă privilegiile sau să se deplaseze în rețea pentru a compromite alte sisteme și conturi în timp ce sunt deghizați în utilizator valid.

Potrivit raportului, este foarte probabil ca actorii sofisticați, inclusiv grupurile infracționale organizate și sponsorizate de stat, să continue să utilizeze instrumente de testare a penetrării și off-the-shelf în viitorul apropiat, deoarece sunt ușor de utilizat și eficiente din punct de vedere al costurilor.

Tacticile noi și sofisticate vizează continuitatea afacerilor

Raportul menționează modul în care un grup cunoscut a vizat în mod agresiv sistemele care susțin Microsoft Exchange și Outlook Web Access și apoi folosește aceste sisteme compromise ca capete de pod în mediul victimei pentru a ascunde traficul, a transmite comenzi, a compromite e-mailuri, a fura date și a aduna acreditări pentru spionaj. Operând din Rusia, grupul, pe care Accenture îl numește BELUGASTURGEON (cunoscut și sub numele de Turla sau Snake), este activ de mai bine de 10 ani și este asociat cu numeroase atacuri cibernetice îndreptate către agențiile guvernamentale, firmele de cercetare în domeniul politicii externe și think tank-uri din întreaga lume.

Ransomware alimentează un nou model de afaceri scalabil și profitabil

Ransomware-ul a devenit rapid un model de afaceri mai profitabil în ultimul an, infractorii cibernetici ducând șantajul online la un nou nivel amenințând că vor elibera public datele furate sau le vor vinde și vor dezvălui identitatea și vor face de râs victimele pe site-uri web dedicate. Infractorii din spatele Maze, Sodinokibi (cunoscut și sub denumirea de REvil) și tulpinile de ransomware DoppelPaymer sunt pionierii acestei tactici în creștere, care generează profituri mai mari și are ca rezultat un val de actori imitatori.

În plus, faimosul ransomware LockBit a apărut la începutul acestui an, care - pe lângă copierea tacticii de șantaj - a câștigat atenție datorită funcției sale de auto-răspândire care infectează rapid alte computere dintr-o rețea corporativă. Motivațiile din spatele LockBit par a fi și ele financiare. Analiștii Accenture CTI au urmărit criminalii cibernetici din spatele acestuia pe forumurile Dark Web, unde se descoperă că fac publicitate actualizărilor și îmbunătățirilor periodice ale ransomware-ului și recrutează în mod activ noi membri promițând o parte din banii de răscumpărare. Succesul acestor metode de extorsiune de tip hack-and-leak, în special împotriva organizațiilor mai mari, înseamnă că acestea vor prolifera probabil pentru restul anului 2020 și ar putea prefigura tendințele viitoare de hacking în 2021. De fapt, analiștii Accenture CTI au observat campanii de recrutare într-un forum popular Dark Web de infractorii cibernetici din spatele Sodinokibi.

Citiți raportul complet Cyber Threatscape 2020 disponibil aici.

Despre Accenture
Accenture este o companie globală de servicii profesionale cu capabilități de top în domeniul digital, cloud și securitate. Combinând experiența fără egal și abilitățile specializate în peste 40 de industrii, oferim servicii de strategie și consultanță, servicii interactive, tehnologie și operațiuni - toate bazate pe cea mai mare rețea din lume de centre de tehnologie avansată și operațiuni inteligente. Cei 506.000 de angajați îndeplinesc promisiunea tehnologiei și a ingeniozității umane în fiecare zi, deservind clienți din peste 120 de țări. Îmbrățișăm puterea schimbării pentru a crea valoare și succes împreună cu clienții noștri, oamenii, acționarii, partenerii și comunitățile. Vizitați-ne la www.accenture.ro.

Accenture Security este un furnizor de top de servicii de securitate cibernetică end-to-end, inclusiv servicii avansate de apărare cibernetică, soluții de securitate cibernetică aplicate și operațiuni de securitate gestionate. Aducem inovații în materie de securitate, la o scară globală și avem o capacitate de livrare la nivel mondial prin rețeaua noastră de centre de tehnologie avansată și operațiuni inteligente. Ajutați de echipa noastră de profesioniști cu înaltă calificare, le permitem clienților să inoveze în siguranță, să construiască reziliența cibernetică și să crească cu încredere. Urmăriți-ne pe @AccentureSecure pe Twitter sau vizitați-ne la www.accenture.com/security. Acest document face referire descriptivă la mărci comerciale care pot fi deținute de alții. Utilizarea unor astfel de mărci în acest document nu este o afirmație a proprietății asupra acestor mărci de către Accenture și nu este menită să reprezinte sau să implice existența unei asociații între Accenture și proprietarii legali ai acestor mărci comerciale.

# # #

Contact de presă Accenture
Bogdan Biszok
Senior Media Associate
M. 0742 100 646
bbiszok@golin.ro