Accenture Report Reveals New Cybercrime Operating Model Among High-Profile Threat Groups

August 14, 2019

Accenture Security's 2019 Cyber Threatscape Report identifies top threats influencing the cyber landscape, including emerging disinformation techniques and evolving relationships in the underground economy

ARLINGTON, Va.; Aug. 14, 2019 – Cybercrime campaigns and high-profile advanced persistent threat groups are shifting how they target victims and focusing more on intricate relationships with "secure syndicate" partnerships to disguise activity, according to the latest 2019 Cyber Threatscape Report from Accenture (NYSE: ACN).

Leveraging Accenture Security threat-intelligence capabilities and research from primary and secondary open-source materials, the annual report provides insights and predictions on the cyberthreat landscape and how it will shift over the next year. The goal is to help organizations stay ahead of threats relevant to their organization, industry and geography.

"Over the past year, cybercriminals have continued to test the resilience of organizations by layering attacks, updating techniques and establishing new, intricate relationships to better disguise their identities, making attribution more difficult to pursue," said Josh Ray, a managing director at Accenture Security. "Organizations should understand the tangible elements, or the bread crumb trail left behind, which can help reveal the motivations, operational procedures and tool use, to create a profile of the adversary. This process is critical for organizations to understand so they can proactively be involved in properly allocating resources and improving their security posture to avoid becoming cybercrime's next victim."

Accenture releases 2019 Cyber Threatscape Report, identifies top threats influencing the cyber landscape and reveals emerging disinformation techniques

A shift in high-profile cybercrime operating models

The report notes a significant increase in threat actors and groups conducting targeted intrusions for financial gain, also referred to as "big game hunting." Despite the arrests of individuals associated with online underground marketplaces, activity among infamous threat actor groups — such as Cobalt Group, FIN7 and Contract Crew — has continued. Accenture Security analysts have also observed the shared use of tools that automate the process of mass-producing malicious documents to spread malware, such as More_Eggs, which is used in both conventional crimeware campaigns and targeted attacks.

The continued activity is associated with relationships forming among "secure syndicates" that closely collaborate and use the same tools — suggesting a major a change in how threat actors work together in the underground economy. With syndicates working together, the lines are even more blurred between threat actor groups, making attribution more difficult.

In addition, Accenture Security analysts have observed a shift in the way Cobalt Group targets victims to gain access to the victims' supply chain networks. While malware has typically been sent to internet users via phishing emails, analysts now see an emergence of malware executed through web browsers focused on targeting online merchants and retailers specifically.

The global disinformation battlefield

The report also finds evidence of a continued global disinformation battlefield influencing social media users and cautions that threat actors are becoming more skilled at exploiting legitimate tools. While disinformation campaigns to influence both domestic or foreign political sentiment and sway national elections will continue, the wider potential impact of disinformation on global financial markets is even more concerning, the report notes.

The financial services industry — and, more specifically, high-frequency trading algorithms, which rely upon fast, text-driven sources of information — are likely to be targeted by large-scale disinformation efforts in the future.

Rise in ransomware: network access for sale

In addition, ransomware is increasingly plaguing businesses and government infrastructures, with the number of ransomware attacks more than tripling in just the past two years. Aside from delivery via spam campaigns, analysts have witnessed threat groups Nikolay and GandCrab planting ransomware directly on networks through network access intrusions. Actors are offering to sell remote desktop protocol (RDP) access to corporate networks, which they've likely gained through compromised servers and RDP brute forcing, to those in underground communities.

To read more about the top threat factors influencing the cyber landscape today and predictions from Accenture Security, please read the full 2019 Cyber Threatscape Report available here .

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions — underpinned by the world's largest delivery network — Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 482,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

Accenture Security helps organizations build resilience from the inside out, so they can confidently drive innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organizations' valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security.

# # #
