Optiv Security Releases Cyber Threat Intelligence Estimate Report to Increase Understanding of Cyber Threat Landscape, Offer Best Practices
Tuesday, October 01, 2019 02:05:00 PM (GMT)

-- Report Finds Many Vertical Industries Still Challenged by Ever-Evolving Cyber Threats --

Businesses and organizations of all sizes have steadily begun to recognize the importance of cybersecurity to their success. As spending and awareness of the importance of cybersecurity increases, so does the demand for intelligence about how best to spend those funds and what security leaders can expect in today's constantly evolving attack surfaces. To help give business leaders insight into the threat landscape to better mitigate risk, Optiv Security has published its 2019 Cyber Threat Intelligence Estimate (CTIE) report, which evaluates the latest cyber threats, explores statistics from various vertical industries, and offers insights into best cybersecurity practices.

"CEOs, corporate board members, CISOs, and other executives have to make cybersecurity 'C-suite business' in order to ensure their companies secure what they have," said General David Petraeus, retired general for the U.S. Army and Optiv Board Member. "Keeping pace requires up-to-date threat intelligence — and the purpose of Optiv's 2019 Cyber Threat Intelligence Estimate (CTIE) is to help business leaders understand the ever-evolving threat ecosystem and employ that knowledge to inform security decisions and investments, continually refining their cybersecurity and risk management programs."

Findings of the report include:

- **Retail, healthcare, government, and financial institutions** continue to be among the most targeted verticals of cybersecurity attacks or attempts among the 10 categories of Optiv clients.
- **Attackers are growing more and more sophisticated**and traditional classifications (nation-states, "hacktivists," or cybercriminals) are becoming somewhat outdated. So called "hybrid threat actors" – who masquerade as a different classification in order to mask their identity – are on the rise.
- **Botnets, Denial-of-Service (DDoS), phishing, and malware** continue to be persistent threats or threat delivery methods, but more modern attack methods and malware delivery systems, such as "cryptojacking" and ransomware, are increasing in popularity.

"We feel it is vital to gather the latest threat intelligence that is actionable and relevant for digestible presentation to for our clients," said Anthony Diaz, vice president and general manager, cyber operations, Optiv. "Business and security leaders can learn from this report and use it to strengthen their security programs. Cybersecurity *can* be an existential threat for organizations, but that only highlights the importance for guidance."

The report lists several best practice recommendations moving forward, including:

- Use multi-factor authentication whenever possible.
- Be proactive, not reactive, when it comes to cybersecurity programs, as bad actors exploit the fact that many organizations only respond to cyber threats instead of actively watching for them.
- Map data access, ideally from an outside perspective in order to better identify possible weaknesses.
- Conduct regular audits of all vendors and other third-party assets and phase out ones that are no longer in use.

"Cyberspace has become more hostile. Hackers are more organized and sophisticated in 2019, and we're seeing malicious attackers increase their counter measures to avoid detection," said Tom Kellermann, Chief Cybersecurity Officer, Carbon Black. "According to our research, no vertical is immune, but the financial industry continues to stand out as a key target for advanced attacks. We hope cybersecurity leaders and teams will use this data as a clarion call to improve their cybersecurity postures."

To access the full report, please visit Optiv's website.

Follow Optiv
Twitter:www.twitter.com/optiv
LinkedIn:www.linkedin.com/company/optiv-inc

Facebook:www.facebook.com/optivinc
YouTube:https://www.youtube.com/c/OptivInc
Blog: https://www.optiv.com/explore-optiv-insights/blog

Optiv Security: Who Secures Your Insecurity?™
Optiv is a security solutions integrator – a global, “one-stop” trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, cyber operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are modernizing cybersecurity to enable clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.

View source version on businesswire.com: https://www.businesswire.com/news/home/20191001005327/en/

--30-- BC/BO

Contact:

Brett Ater
(913) 304-7683
Brett.ater@optiv.com
or
Jason Cook
(816) 701-3374
Jason.cook@optiv.com

Industries: Software, Networks, Internet, Data Management, Technology, Security
Languages: English
Primary Identifiers: KKR-US
Related Identifiers: KKR-US
Source: Optiv Security
Subjects: Product/Service