ANALYSIS:

Dark web research highlights increased professionalisation and collaboration among cyber criminals

9th August 2022 | Andrew Staniforth | Policing Insight

Picture © thomaguery / iStockphoto

A new study into the evolution of cybercrime on the dark web has highlighted an increasingly professional approach from criminals, with greater collaboration, the packaging of tools and services, and a buoyant online market; but as Policing Insight's Andrew Staniforth reports, businesses and organisations can use similar collaborative techniques to improve their own cybersecurity.

A new study of cybercrime on the dark web has highlighted the rising volume of criminal activity, the professionalisation and collaboration of cybercriminals, and the cheap entry point into the illicit market – with more than three-quarters of malware available for less than $10.

> "Vendors are selling products in bundles, with 'plug and play' malware kits, malware as a service, tutorials and mentoring services all reducing the need for technical skills and experience to conduct attacks."

The independent *Evolution in Cyber Crime* report also found that vendors are selling products in bundles, with 'plug and play' malware kits, malware as a service, tutorials and mentoring services all reducing the need for technical skills and experience to conduct attacks.

The report, which was carried out by the dark web investigation company Forensic Pathways and published last month, analysed 33,000 active websites across the dark web, including 5,502 forums and 6,529 marketplaces.

Between February and April 2022, analysts identified 17 recently active cybercrime marketplaces across the Tor network and 16 hacking forums.

Commissioned by HP Wolf Security, the study also traced the key cybercrime moments and trends over the last 30 years, detailing the dynamics of underground markets today and where they might be headed, and what organisations can do to bolster their defences.

The key findings make for stark but essential reading for all in authority engaged in combatting cybercrime and improving cyber security, and underline the need for greater collaboration to tackle all manner of cyber risks across the cyber security sector

Reality of risk

This latest research was carried out against a background of booming cybercrime; between 2008 and 2021, the FBI recorded a 207% increase in cybercrime reports, with losses hitting almost $7bn last year.

The continued rise in cyber threats is being driven by an increasingly professionalised, specialised, and collaborative underground supply chain that is harming individuals and businesses alike.

> "The report also identified the "irony of honour" among cyber thieves; much like the legitimate online retail world, trust underpins cybercriminal commerce between buyers and sellers."

The HP Wolf Security report identified that cybercrime goods and services are both cheap and plentiful; 76% of advertisements for malware and 91% for exploits are listed for under $10, and the average cost of compromised Remote Desktop Protocol credentials is just $5.

Alongside the increasingly professional 'packaging' of cybercrime bundles, the report also identified the "irony of honour" among cyber thieves; much like the legitimate online retail world, trust underpins cybercriminal commerce between buyers and sellers

More than three-quarters (77%) of cybercriminal marketplaces analysed require a vendor bond – a license to sell – which can cost up to $3,000, while 85% of these marketplaces use escrow payments, and 92% offer dispute resolution services. Every marketplace analysed also provides vendor feedback scores. Given the risk of law enforcement takedowns and disruption by rivals, cybercriminals can stay a step ahead by transferring reputation between marketplaces, as the average lifespan of a dark web website is only 55 days.

The report reveals that vulnerabilities in popular software are providing cybercriminals with a foot in the door, focusing on exploiting known bugs in popular software that will allow them to gain a foothold and take control of systems.

Examples include the Windows operating system, Microsoft Office, web content management systems, and web and mail servers. Niche exploits of specialised systems command higher prices (typically from $1,000-$4,000) on markets; zero days (vulnerabilities that are not yet publicly known) are retailing at tens of thousands of dollars.

Enterprise evolution

> "The investigators warn of a potential growth in extortion attacks using the threat of data destruction against sectors that depend on IoT devices – particularly those who rely on infrastructure in time-sensitive and critical ways, which includes much of the public sector and emergency services."

The report underlines that the future cybercrime threat landscape is bleak, with destructive attacks potentially becoming even more damaging; and as organisations embrace digital transformation and the Internet of Things (IoT), attackers will likely take advantage of the "ever-widening attack surface" these create. The investigators warn of a potential growth in extortion attacks using the threat of data destruction against sectors that depend on IoT devices – particularly those who rely on infrastructure in time-sensitive and critical ways, which includes much of the public sector and emergency services.

Moreover, intrusions are likely to become more professionalised and targeted. To maximise the value of their intrusions, cybercriminals will continue to adopt the tactics of advanced persistent threats (APTs), such as spending longer on target reconnaissance and establishing long-term access within networks. Emerging technologies such as Web3 could also open new opportunities to create reputation systems that support the cybercrime economy, and which may be harder for the authorities to take down.

Quantum computing could be deployed to supercharge decryption efforts, and when combined with cyber attackers focusing on making their attacks more efficient, this significantly amplifies future cyber risks becoming reality.

A new hope

Set against cybercrime backdrop of growing collaboration, specialisation and professionalisation among hostile cyber actors, the report offers some hope for the future, providing a series of essential steps to be taken by organisations to reverse the rising tide of cyber threats. Planning for the worst-case scenario is recommended as a key priority for preparedness, resilience, and recovery. The report suggests that as well as developing and installing cyber defences, focus on business continuity in the event of an attack is vital; by preparing in advance and anticipating what tactics attackers might use, organisations can recover more quickly.

> "One of the biggest reasons for hope is seeing how the cybersecurity community has grown in its size and willingness to share. Much like adversaries, collaborating and sharing knowledge is essential for fighting back against the tide of attacks."
>
> **Alex Holland, Senior Malware Analyst, HP Inc**

Organisations must also learn to limit the risk posed by insider threats, from the very people employed and partners engaged in delivering their business and services, recommending that organisations should have processes in place to vet supplier security and educate their workforce about social engineering. The HP Wolf Security report also recommends a culture shift from being process-orientated to practice reactions. Robert Masse, HP Security Advisory Board member and Partner at Deloitte explained: "We need to shift away from monitoring statistics and focus more on winning the game. You can have a team with exceptional stats and solid players, but what matters is: can they win when it counts."

Alex Holland, Senior Malware Analyst at HP Inc, added: "One of the biggest reasons for hope is seeing how the cybersecurity community has grown in its size and willingness to share. Much like adversaries, collaborating and sharing knowledge is essential for fighting back against the tide of attacks. By proactively scanning the landscape for threats and sharing insights with our peers, we can together build a more secure and resilient digital world."

Link to online article at Policing Insight: https://policinginsight.com/features/analysis/dark-web-research-highlights-increased-professionalisation-and-collaboration-among-cyber-criminals

Andrew Staniforth is Director of Innovation at SAHER (Europe), a security research, training and consultancy operating at a global level, participating in the NOTIONES (*iNTeracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS*) network, funded by the European Commission Horizon 2020 Programme (No. 101021853). Andrew is also an active Researcher of Cyber Threats at the Hillary Rodham Clinton School of Law and Criminology, University of Swansea. As a former Counter-Terrorism Detective, he has worked across the world and supported missions of the United Nations Terrorism Prevention Branch. **Contact:** Andy@saher-eu.com
To learn more about NOTIONES visit: https://www.notiones.eu