CALL FOR EVIDENCE RESPONSE

Joint Committee on the National Security Strategy Inquiry into Ransomware

Zeki Turedi
CTO EMEA
CrowdStrike

December 16, 2022

I. INTRODUCTION

In response to the Joint Committee on National Security Strategy's (JCNSS) call for evidence on its new inquiry into ransomware, CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international cybersecurity provider that defends globally distributed enterprises from globally distributed threats. We directly support organisations of all sizes, public and private, in the UK and help them identify, prevent, and defend themselves against cyber threats. Moreover, this perspective is informed by CrowdStrike's recent participation alongside the UK government in the International Counter Ransomware Initiative's Summit at the White House.

CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in responding to and protecting organisations from data breaches and a variety of other cyber threats.

II. COMMENTS

We appreciate JCNSS's engagement efforts - including this call for evidence and the committee meeting on ransomware that invited sector experts - to reach a variety of stakeholders throughout this process. We have included responses to specific topics in the call for evidence, along with general observations and comments that may be useful as the UK addresses this serious problem.

A. The extent and nature of the ransomware threat (including sources), modes of extortion, and how the threat could evolve in future.

In the last 24 months we have observed a shift in criminal cyber activity ("eCrime"). The opportunistic victimisation of businesses during COVID-19 has now transitioned into lucrative, sustained targeting of vulnerable organisations by a highly capable and sophisticated network of threat actors targeting essential entities for monetisation. Unfortunately, this trend shows no signs of decreasing. As of today we see eCrime targeting nearly all sectors, with the key focus of Telecommunications, Technology, Finance, and Government. Worryingly, Healthcare is also a large and growing target across Europe.

Threat actors are increasingly adapting ransomware campaigns to incorporate more explicit threats of data extortion. In addition to encrypting enterprise networks in order to disrupt or halt operations, attackers increasingly threaten to publicly leak stolen data, from sensitive business information and intellectual property to internal communications and customer data. This means that in addition to slowing or stopping productivity, these threat actors are purposefully attempting to hold victims at heightened risk of reputational damage and adverse regulatory impacts.

As an evolution, the threat actor is becoming quicker, more agile and brazen when targeting entities. The entry barrier for a ransomware operator to get started has been considerably lowered as of recent, with the development of very successful Ransomware as a Service offerings, where Ransomware technology can be purchased or leased on a commision basis from more sophisticated groups to lesser capable groups, with powerful tools that automate the complex steps of targeting a victim.

Ransomware operators are considerably out-pacing victim organisations' under-funded, overworked security and IT teams who are typically prevented from adequately protecting their business or organisation from the threats of today due to internal policy complexities, a lack of investment in security, or incentives to use yesterday's security technologies.

B. Levels and sources of vulnerability of UK organisations to ransomware, including operators of critical national infrastructure.

ECrime threats, including ransomware in particular, are increasing globally. UK organisations are not inherently more vulnerable to this threat activity than comparably developed anglophone nations. Still, like other countries, we must strengthen defences and remain alert.

Cyber threats are often expressed along geopolitical lines. Threat actors in Russia in particular may increasingly target Western entities—including within the UK—in light of heightened political tensions and the mounting effects of sanctions. Critical infrastructure operators in particular are heavily targeted given their centrality to day-to-day life, and their corollary sensitivity to disruption. Recent, high-profile ransomware campaigns, such as the attack on NHS, have the potential to cause severe social disruptions and carry broader domestic political implications.

C. The UK victim experience, including sources of support for prevention, detection and recovery, public-private partnerships, the role of the media, access to and availability of insurance cover, and regulatory requirements placed on ransomware victims.

ECrime groups not only look to target and disrupt the networks of the victims, they also increasingly look to impact people. As noted above, this includes holding personal data at risk with the threat of releasing stolen confidential information and targeting Critical Infrastructure operators that could disrupt a whole sector. Additionally, the cybersecurity threat to small- and medium-sized businesses (SMBs) continues to grow as criminals recognise how vulnerable they can be, and the potential value of the data they have. Today's attackers have their sights set on SMBs and nonprofit organisations — and the consequences can be devastating as the cost of these incidents rises into the millions.

D. The effectiveness of the response to ransomware by Government, law enforcement agencies and other UK state actors, including key operational challenges and ministerial oversight.

Oftentimes, proposals to solve ransomware focus on post-incident remedies. For example, government organisations may provide investigational support after an organisation has already become a victim. Similarly, in the UK, CrowdStrike has observed organisations focussing their ransomware strategy on obtaining cyber insurance coverage - like the former, an approach that is only implemented once an organisation has been victimised.

Governments alone cannot solve for and protect from eCrime, similarly the focus should not be on post-incident resolution or response. Increasingly, significant cyber attacks for organisations big and small begin with the exploitation of credentials, whether through harvesting a username and password or by taking advantage of inherent flaws in identity architecture to permit an adversary to move laterally throughout a network. Accordingly, the government can play a role in showcasing best practices related to identity protection as well as incentivising the adoption of best-in-class technologies. Beyond merely advocating for multi-factor authentication, the UK government should adopt and promote Zero Trust security architectures to move beyond the status quo of networks predicated upon inherent trust and low friction movement for adversaries or encryption of assets.

Fundamentally, it is inherent for organisations to have visibility into their networks in order to detect and respond to ransomware and to adopt measures that reduce risk throughout an attack killchain. This means the UK government, like the European Union via the ENISA State of the Art Guide and the United States in its May 2021 Executive Order on Cybersecurity, should mandate government use of and incentivise private sector adoption of modern cybersecurity techniques such as Endpoint Detection and Response (EDR), Log Management, Threat Hunting, and Identity Protection. This, coupled with basic cyber hygiene can make a meaningful impact pre-breach and post-incident. Some of the core best practices to enhance cyber hygiene include creating adequate backups, having an incident response plan in place, having an incident response provider on retainer to offer immediate help. Security approaches designed to protect against threats, actively hunt for threats, and create preparedness in the event of an incident, can make a meaningful impact in protecting UK organisations against ransomware.

E. Reforms that might enhance the UK's resilience to ransomware, reduce the economic and societal damage that it causes, and/or support the law enforcement response.

These eCrime actors can be stopped, but this will require holistic efforts from the public and private sectors. The public sector, for example, can continue to facilitate collaboration, promote best practices, and strengthen enforcement measures. We also think it's appropriate to review all mechanisms to increase the adoption of cutting-edge security solutions–particularly within CNI. Organisations that utilise Endpoint Detection and Response tools, leverage Managed Security Services where appropriate, and have implemented strong Identity Protection capabilities are immeasurably better protected than those that rely on legacy protections.

F. The scope for international cooperation to combat the global ransomware threat more effectively, including on crypto-currency regulation.

International cooperation is necessary to tackle eCrime given that it is such a global issue. Recently, the United States hosted the International Counter Ransomware Initiative Summit, in which the UK and CrowdStrike participated. There were many positive commitments following the Summit to build out long-term cooperation between the 37 countries that participated. We recommend the countries involved follow through with the commitments such as creating an International Counter Ransomware Task Force, increased information sharing, and engaging with the private sector to continue the momentum from the Summit.

The UK is in a unique position as the policy plank holder for the Initiative, which provides an opportunity to incentivize the adoption of technologies and processes that increase resiliency against ransomware and raise the costs for adversaries. As an international community, we should be more aggressive about disrupting threat actor operations. This likely includes more proactive steps to take down malicious domain names and associated infrastructure. CrowdStrike recommends the UK, along with allies, find ways to coordinate more purposefully on this front.

There is an open debate as to whether ransomware payments should be permitted so long as they are not to sanctioned parties or completely banned so as not to potentially incentivise criminal enterprise. Regardless of how the debate resolves itself, it can be expected that eCrime actors will continue to innovate, using payment methods and infrastructure with the lowest points of friction and cost of doing business. Government is in a unique role to disrupt adversary infrastructure by leveraging open source domain name registration, blockchain ledger information, and data shared from traditional financial institutions.

G. Lessons that could be learned from other countries' approaches and responses to ransomware.

Strengthening public sector cybersecurity posture makes the government more resilient and ensures continuity of services. In the U.S., recent initiatives such as the May 2021 Executive Order on Cybersecurity, which requires the Federal government to implement Zero Trust architectures; strengthen logging capabilities; and deploy Endpoint Detection and Response (EDR) technology, may serve as a useful model to the UK. We recommend that the JCNSS continue consulting with the expert community and strengthen cybersecurity oversight within this and other relevant Parliamentary Committees.

III. CONCLUSION

JCNSS's call for evidence on ransomware represents an important step to countering this significant cyber threat. We hope that industry stakeholders have continued opportunities to voice comments in any lines of work that come from this call for evidence. Finally, because the underlying technologies and adversary TTPs evolve faster than law and policy, we recommend and emphasise that any legislative updates and proposed rulemaking focus on principles, where appropriate, rather than prescriptive requirements and include mechanisms for periodic review, updates, and revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made directly to the author or to: policy@crowdstrike.com

***