IAB COVID-19 Network Impacts

Position paper for workshop 2020

Introduction

Advanced Persistent Threat (APT) groups and cyber criminals are exploiting the COVID-19 pandemic. These cyber threat actors will often masquerade as trusted entities; their activity includes using coronavirus-themed phishing messages or malicious applications; their goals and targets are consistent with long-standing priorities such as espionage and information operations. Cyber criminals are using the pandemic for commercial gain, deploying a variety of ransomware and other malware.

Attackers are using COVID-19 related scams and phishing emails to target: individuals, small and medium businesses, large organisations, and organisations involved in both national and international COVID-19 responses[i] (healthcare bodies, pharmaceutical companies, academia and medical research organisations[ii]). At the same time, the surge in home working has increased the use of and dependence on VPNs, some of which include remotely exploitable vulnerabilities[iii], providing a larger attack vector that has been leveraged against individuals and organisations[ii].

Of all scams detected by the UK NCSC[iv] that were purporting to originate from UK Government, more related to COVID-19 than any other subject[v]. Although, from the data seen to date, the overall levels of cyber crime have not increased, both the NCSC and CISA[vi] are seeing a growing use of COVID-19 related themes by malicious cyber actors.

This position paper describes an overview of COVID-19 related malicious cyber activity and outlines questions for the IETF posed by these challenges. The original security advisory[v,] from which this content is drawn, also offered practical advice for individuals and organisations to reduce the risk of being affected, and included Indicators of Compromise based on analysis from CISA, NCSC, and industry.

The increased threats and network security impacts arising from COVID-19 fall into two areas: (1) the agility of malicious actors to spin up new campaigns using COVID-19 as a lure, and (2) the increased threat surface from a rapid shift towards home working. Both risk areas are network impacts directly resulting from the COVID-19 pandemic, rather than an increase in internet usage more generally.

Cyber attacks and network engineering

Both APT groups and cyber criminals are likely to continue to exploit the COVID-19 pandemic over the coming weeks and months. Threats already observed include:

- Phishing, using the subject of coronavirus or COVID-19 as a lure
- Malware distribution, using coronavirus or COVID-19 themed lures
- Registration of new domain names containing coronavirus or COVID-19 related wording
- Attacks against newly (and often rapidly) deployed remote access or remote working infrastructure

Given the large numbers of people working from home and the increased activity and number of malicious cyber actors exploiting the COVID-19 pandemic, there should be strong interest from the internet community in how to make such attacks harder to execute, easier to detect and prevent, or a combination of both. From this list of threats, most can be improved or worsened by protocol engineering: detection of malware distribution systems that use internet infrastructure, prevention of domain registration and takedown of domains used for malicious purposes, and mitigations against phishing (making it harder for attackers to reach users).

1. **What IETF engineering has already helped to protect users and improve security against these attacks?**

Attacks and defences

Attacks: Social engineering techniques

Malicious cyber actors often rely on basic social engineering methods to entice a user to carry out a specific action, taking advantage of human traits such as curiosity, concern and the desire to be helpful. Though not fundamental to all malicious cyber activity, social engineering is incredibly common, even among sophisticated actors. The recently published RFC 8890 states that IETF decisions should favour end users. In a pandemic situation and times of uncertainty, even users with strong technical skills experience curiosity and concern; indeed, it could be argued that most users are more vulnerable to these manipulative techniques.

2. **What does the pandemic situation amplify or reduce in RFC 8890 and other user-specific initiatives?**

Phishing is the most well-known social engineering technique, and NCSC guidance[vii] recommends a four-layered approach to tackle it. The first defence layer is "make it difficult for attackers to reach your users" and the second layer is "help users to identify and report suspected phishing emails". In the midst of the pandemic, the NCSC launched its Suspicious Email Reporting Service[viii]. This initiative directly addresses the second layer and indirectly addresses the first layer, by protecting more vulnerable users with reports from vigilant users.

Since its launch on 21st April 2020, up to 30 September 2020, 2,390,000 reports had been received through this service, resulting in the removal of 13,291 scams and 30,344 URLs.

3. **Given reduced user vigilance to phishing in a pandemic situation and in isolated working environments, and a longer-term shift in working patterns and locations, what protocol-level work can be started to make it difficult for attackers to reach users?**

Malicious actors have used COVID-19 themes to persuade victims to click on a link or download an app that leads to a phishing website or the downloading of malware. For example, a malicious Android app that purports to provide a real-time coronavirus outbreak tracker instead attempts to trick the user into providing administrative access to install 'CovidLock' ransomware on their device[ix]. To create the impression of authenticity, email sender information may be spoofed to appear to come from a trustworthy source, such as the World Health Organization (WHO) or an individual with 'Dr.' in their title[x]. Attackers have also encouraged users to open files (such as email attachments) that contain malware, for example using email subject lines that contain COVID-19 related phrases such as 'Coronavirus Update' or '2019-nCov: Coronavirus outbreak in your city (Emergency).' These malicious attachments may be named with COVID-19 related themes, such as "President discusses budget savings due to coronavirus with Cabinet.rtf". Other examples purport to be from an organisation's human resources (HR) department and advise the employee to open the attachment.

Attacks: Remote working infrastructure

COVID-19 saw an increasing number of organisations and individuals turning to communications platforms (such as Zoom and Microsoft Teams) for online meetings and working from home. In turn, there was an increase in malicious cyber actors hijacking online meetings that are not secured with passwords or that use unpatched software as another attack vector[x].

Many enterprises turned to VPNs for homeworking, to encrypt data from their clients to the enterprise. Some organisations did this for the first time; others put their established solutions under much greater load. APT29 was successful in using recently published exploits in a range of VPN software to gain initial footholds[Error! Bookmark not defined.], including but not limited to: CVE-2019-19781 Citrix[xi], CVE-2019-11510 Pulse Secure, CVE-2018-13379 FortiGate[iii] and CVE-2019-9670 Zimbra[xii]. These attacks by APT29 were targeted against organisations involved in COVID-19 vaccine development, highlighting the potential consequences of vulnerable infrastructure.

Use of Microsoft's Remote Desktop Protocol (RDP) for remote working was another popular solution, with large increases in RDP endpoints exposed to the Internet[xiii]. This left many instances open to attack, either through RDP vulnerabilities (e.g. BlueKeep[xiv]) or password brute force attacks.

4. **What protocol design and deployment decisions can be taken to reduce vulnerability of remote working infrastructure?**

Defences: Indicators of Compromise

User education can help combat both social engineering techniques and attacks on remote working infrastructure, either through preventing users being caught by phishing or by ensuring that remote working infrastructure is used in a secure manner. However, as outlined above, user education is not sufficient and likely to be less effective during a pandemic. Combating a range of attacks that include such convincing social engineering efforts requires a layered approach.

Attachments, fields, links and other artefacts found in the investigation of cyber attacks are collectively known as 'Indicators of Compromise' (IoCs)[xv]. In response to the COVID-19 attacks, a non-exhaustive list of COVID-19 related IoCs[xvi] was published, including protocol artefacts, allowing the rapid sharing of threat information. This allows other defenders to discover the same indicators and deploy them at scale, for example in network and endpoint security solutions, to block malicious activity and hence prevent these scams. The speed, scale and efficacy that IoCs allow incident responders make IoCs vital to prevention and detection of these attacks, particularly in a distributed working environment without traditional enterprise network defences. The extent to which IoCs have mitigated such a range of social engineering attacks during the COVID-19 pandemic is testimony to how invaluable they are for cyber defence.

5. **What IETF engineering, IRTF research and future initiatives would make it harder for the same wave of attacks to happen in future?**

Conclusion

Malicious cyber actors are continually adjusting their tactics to take advantage of new situations, and the COVID-19 pandemic is no exception. Malicious actors use the high appetite for COVID-19 related information as an opportunity to deliver malware and ransomware and to steal user credentials. Individuals and organisations should remain vigilant. For genuine information about the virus, individuals and organisations need to use trusted resources such as, for UK residents, the UK government website, Public Health England or NHS websites.

Against the landscape of a shift to working from home, an increase in user vulnerability, and IT departments often overwhelmed in rolling out new infrastructure and devices, IoC sharing was a vital part of the response to COVID-19 related scams and attacks. It's unsurprising that the security sector saw and felt the network security impact of the COVID-19 crisis, as much as or even more than sectors that worked to ensure performant connections and reliable infrastructure. Against the backdrop of the COVID-19 crisis, tireless work was done by the security industry to protect users and the most vulnerable in our societies.

The COVID-19 crisis showcased the agility with which malicious actors can move, and the vast potential of the disruption and damage that they can inflict. Equally, it showed the agility of defenders, when they have access to the tools and information they need to protect users and networks, and showcased the power of IoCs when defenders around the world are working together against the same problem.

[i] https://www.ncsc.gov.uk/files/Joint%20NCSC%20and%20CISA%20Advisory%20APT%20groups%20target%20healthcare%20and%20essential%20services.pdf

[ii] https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

[iii] https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities

[iv] UK NCSC: United Kingdom National Cyber Security Centre

[v] https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory

[vi] CISA: Department for Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency

[vii] https://www.ncsc.gov.uk/guidance/phishing

[viii] https://www.ncsc.gov.uk/information/report-suspicious-emails

[ix] https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware

[x] https://www.ncsc.gov.uk/files/Final%20Joint%20Advisory%20COVID-19%20exploited%20by%20malicious%20cyber%20actors%20v3.pdf

[xi] https://www.ncsc.gov.uk/news/citrix-alert

[xii] https://nvd.nist.gov/vuln/detail/CVE-2019-9670

[xiii] https://blog.reposify.com/127-increase-in-exposed-rdps-due-to-surge-in-remote-work

[xiv] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

[xv] https://datatracker.ietf.org/doc/draft-paine-smart-indicators-of-compromise/

[xvi] CSV file of IoCs: https://www.us-cert.gov/sites/default/files/publications/AA20- 099A_WHITE.csv