Special Bulletin – Ukraine/Russia Conflict - Cyber Security Briefing

Prepared by: Mike Bluestone & Neil Shanks

Date: February 2022

CORPS SECURITY

Special Bulletin: Cyber Security

The risk to the UK posed by the current situation between Russia and Ukraine may not follow the traditional route of previous conflicts. Whilst there is a very real physical threat to those near the Ukrainian/Russian border, as well as neighbouring countries (such as Poland) being poised for potential clashes, the risk to other leading NATO countries may come in a different format. Russia has demonstrated their cyber threat capabilities several times on the global stage in recent years, not least in the December 2015 attack on power stations around Kiev by "Sandworm" (a branch of the GRU a.k.a. Glavnoye Razvedyvatel'noye Upravleniye, the Russian Intelligence Directorate) which resulted in power outages. Sandworm is also believed to have been involved in the targeting of NATO states ahead of the 2019 European Union elections. Russia have a long history of state sponsored espionage and engage a number of groups to undertake hacking operations on their behalf, including Sandworm, Cozy Bear, Fancy Bear, Wizard Spider, and potentially DarkSide (DarkSide claim to be apolitical). This list is not exhaustive.

Whilst the 2015 attack in Kiev aimed to cause disruption, the targeting of utility providers could prove to be far more damaging. An attack on the water treatment plant in Oldsmar, Florida in February 2021, as reviewed in the March 2021 Corps Relay, is an example of an attack with another motive (please note there is no suggestion that Russia was involved in this attack). In the Oldsmar incident a Cyber Attacker raised the sodium hydroxide in the water to 111 times the normal level, which is dangerous to human life, but fortunately the change was identified before any harm was caused. In addition to this, DarkSide, who are believed to be a Russian hacking group, were responsible for a ransomware attack on the Colonial Pipeline in the US in 2021. The fuel shortages that resulted from the attack resulted in the Federal Motor Carrier Safety Administration (FMCSA) declaring a state of emergency across 18 states.

Where causing disruption to the population and business is the goal there are a number of targets other than utilities that can be selected. On a larger scale, the targeting of key services supporting the functionality of the internet and businesses, including data centres, could prove attractive. Targeting cloud edge platforms, which help reduce the latency/delay when using apps/internet sites, could be one simple way to cause mass disruption through hitting a single point. An example of the potential impact of this was seen in June 2021 when the Fastly service went down resulting in many sites (including Amazon, eBay, and the .Gov website) being inaccessible. The Fastly incident, and some information on the UK's Cyber Security Plans, were discussed in the July 2021 Corps Relay.

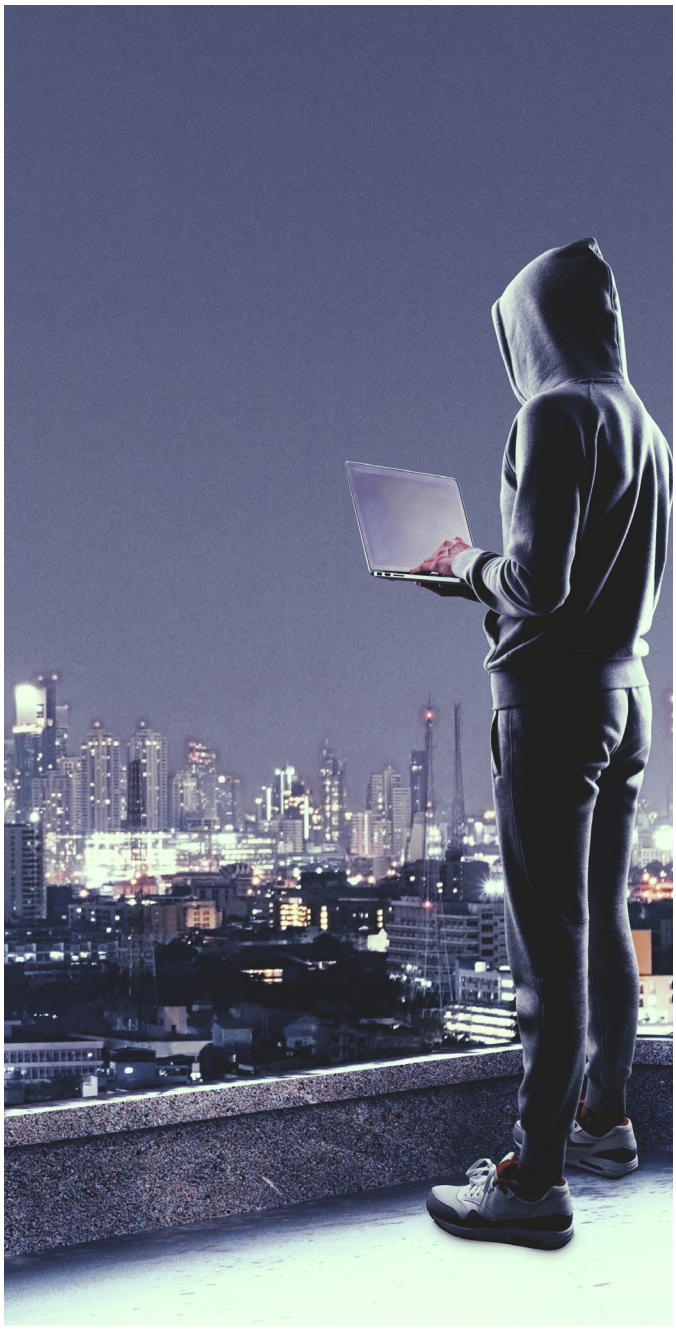
On a smaller scale, attacks on individual websites or networks can be orchestrated fairly simply through the use of Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks. These attacks use multiple machines to flood websites/networks in order to make them run too slowly to fulfil their intended function. Malware. Rootkits, and Internet of Thigs (IoT) attacks are other common methods used by hackers to target businesses, with the first two of the three often being spread by "Phishing".

Phishing is the process of sending a fraudulent communication that is designed to appear as if it is from a reputable source, which will seek to get someone to allow access to their system. Methods of gaining access to the system may be by getting recipients to download malicious software (e.g. Malware or Rootkit) or by clicking a link that either downloads malicious software or takes them to a fraudulent website that aims to get the recipient to input sensitive information (e.g. username, password, financial data etc.). Some Phishing emails will try to get you to visit websites via links and may claim that this must be completed to reinstate the users access to a named site. Cyber Criminals may use a website being down (possibly as a result of their own attack) as an opportunity to attack users. A good site to check whether there is a reported issue on a commonly used site (e.g. Facebook) is DownRightNow (alternatives are available and we do not endorse the use of a single source for cyber security data). If this is the case, wait until the site is reported as being "Up" before trying to use it again.

Special Bulletin – Ukraine/Russia Conflict Cyber Security Briefing
February 2022

Whilst businesses and individuals can't do a lot to prevent attacks on national infrastructure (including cyber infrastructure), they can take steps to ensure their own cyber security provision is robust. Recently updated and published guidance for business, from the National Cyber Security Centre (NCSC), on actions to take when the cyber threat is heightened provides advice and information on steps that businesses should be taking at this time. The NCSC also provide a range of additional information through their website. In addition to the NCSC guidance, please see below for some general guidance on how to avoid falling foul of a Phishing attack:

- If you are not expecting an email from a sender with attachments, please always be wary of this – contact the customer by phone from an independently verified number (not the one from the email) and ask for them to confirm they sent the email
- Avoid clicking on unknown links – Do not assume that the link goes to where it says it does – hover the cursor over the link and it will reveal the real link destination – example of how a false link can look below (this appears to send you to FalseLink.co.uk but actually takes you to the Corps Relay archives): https://www.FalseLink.co.uk
- A phishing email may have spelling errors in the subject and body of the email
- Check the email address is correct – again, check for spelling errors and that the structure is the same (e.g. name@corpssecurity.co.uk and not name@CorpSecurity.co.uk), as well as that the top level domain (e.g. .com, .org., .co.uk etc.) is what you would expect
- Domains can be bought that are very similar to the legitimate one being used (e.g. CorpsSecurity.com or CorpsSecurity.co.uk) for both emails and websites. Check this is what is expected and, if in doubt, do not reply/click anything
- Websites like WhoIs allow you to see when a domain was established. If it is a company that has been around for a long time it is unlikely they would have a website that is very recent (tip – it also gives details of similar domains that are taken or available, one of which might be the legitimate one that is being mirrored)
- Legitimate emails will not ask you to provide sensitive information
- **In all instances, if you are in doubt:**
  - **Do not open any attachments or links**
  - **Inform your IT/Cyber Security Department immediately**
  - **Clearly mark the email as a suspected phishing email when sending to your IT/ Cyber Security Department**
  - **Do not share the email with anyone else**
  - **Do not save the email**
  - **Permanently delete from your system if asked to do so (including from your deleted items folder)**



Market House
85 Cowcross St
London
EC1M 6PF

07890 590352
Neil Shanks

intel@corpssecurity.co.uk
www.corpssecurity.co.uk