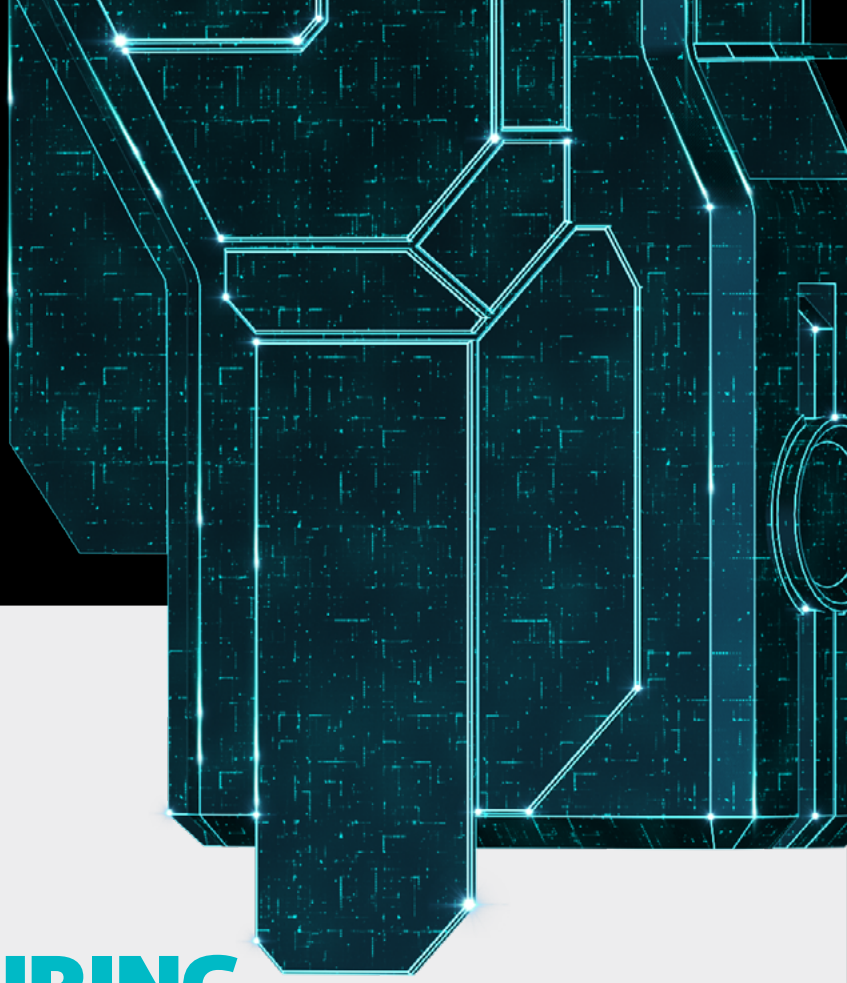
CYBERSECURITY
EXPERTS ON YOUR SIDE



RDP: CONFIGURING SECURITY FOR A REMOTE, BUT NOT DISTANT FUTURE

Leveraging RDP to manage your network through a crisis? Then make sure you are limiting your risk with good practice, authentication tools and by leveraging the existing knowledge base.

The corona pandemic has pushed enterprises around the world to send their people home and mass-leverage remote work using any means possible. This includes the use of RDP technology, which in the past few years has been subject to abuse. Numerous instances have emerged, especially when attackers have found ways to exploit poorly configured settings or weak passwords to gain access to company networks.

Once inside, attackers have an open door to do almost anything including, for example, the theft of intellectual property or other sensitive information and encrypting it for ransom.

AUTHOR:Aryeh Goretsky
CONTRIBUTOR: James Shepperd

April 2020

1.

What do attackers do with RDP?

In the past few years, ESET has seen an increasing number of incidents where attackers connected remotely to Windows Servers from the internet using RDP and logged on as the computer's administrator. This implies various vectors including: vulnerabilities (such as BlueKeep CVE-2019-0708), phishing, credential stuffing, password spraying, brute force, or poorly configured access to internal systems.

Once attackers are logged into a server as an administrator, they will typically perform some reconnaissance to determine what the server is used for, by whom and when it is being used. Then they can begin performing malicious actions.

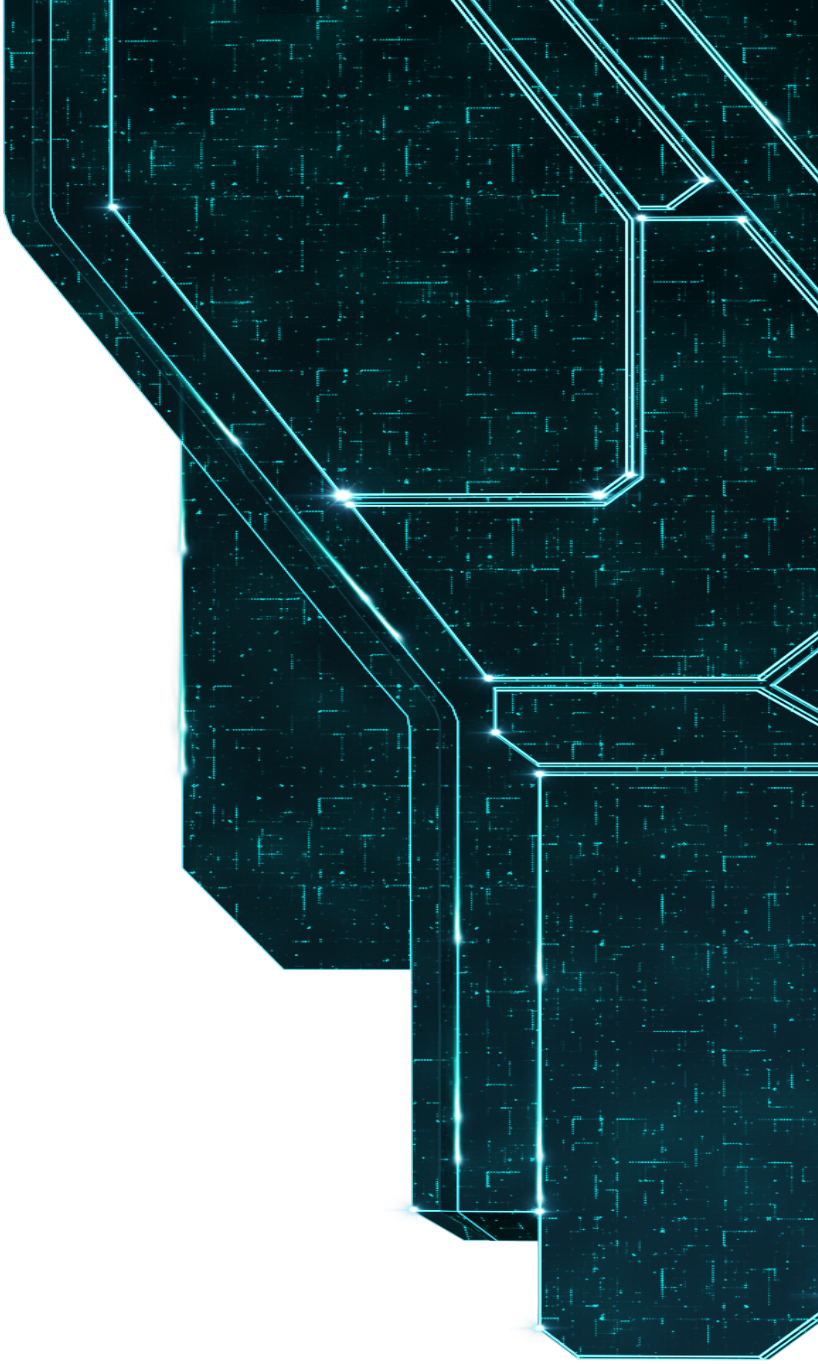
This is not a complete list of all they can do, nor are they necessarily going to perform all of these activities. The exact frequency, sequence and nature of what attackers will do varies greatly.

COMMON MALICIOUS ACTIVITIES WE HAVE SEEN INCLUDE:

- clearing log files containing evidence of their presence on the system
- disabling scheduled backups and shadow copies
- disabling security software or setting up exclusions in it (which is allowed for administrators)
- downloading and installing various programs onto the server
- erasing or overwriting old backups, if they are accessible
- exfiltrating data from the server

THREE OF THE MOST COMMON ARE:

- installing coin-mining programs in order to generate cryptocurrency, such as Monero
- installing ransomware in order to extort money from the organization, often to be paid using cryptocurrency, such as bitcoin
- in some cases, attackers might install additional remote-control software to maintain access (persistence) to compromised servers in case their RDP activities are discovered and terminated



NOTABLE AND RECENT MALICIOUS RDP ACTIVITY

One prolific ransomware, GandCrab, which operated until May 2019, used a Ransomware-as-a-Service (RaaS) business model in which the developers leveraged a number of affiliate malicious actors to further distribute the malware. GandCrab, in particular, targeted MSPs using RDP to connect to their remote management tools and extort multiple customers at once.

Though GandCrab's ransomware operators announced their retirement after the FBI released keys to decrypt their ransomware, our experts think that GandCrab source code may have been sold to a different group that is now running Sodinokibi, (due to changes in the code, its structure and subsequent updates). Sodinokibi ransomware appeared just as GandCrab started to suspend their operations, essentially replacing GandCrab and using similar tactics, techniques and procedures as their predecessor to target MSPs via RDP.

The MSP connection is notable for enterprises too, as MSPs hold the 'keys to the kingdom' for thousands of SMBs (and those SMB's business relationships), and even some enterprises. On the MSP client side, businesses face similar dependencies as both teams and individual users depend on admins for help with everything from licensing and updates to security.

RDP VULNERABILITY OPENS A BIG DOOR TO RISK

Attacks via RDP have been slowly, but steadily, increasing and subject to a number of governmental advisories from the FBI, the UK's NCSC, Canada's CCCS, and Australia's ACSC, to name a few.

In May 2019 the floodgates opened with the arrival of CVE-2019-0708, aka "BlueKeep", a security vulnerability in RDP affecting Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 and Windows Server 2008 R2*.

While these may be legacy systems, and in most cases are either no longer supported or only have limited vendor support, telemetry suggests there will be many vulnerable systems still in use.

The BlueKeep vulnerability allows attackers to run arbitrary program code on their victims' computers. While even individual attackers can be a widespread threat using automated tools for attacks, this vulnerability is "wormable," which means an attack could spread itself automatically across networks without any intervention by users, just as the Win32/Diskcoder.C (aka NotPetya) and Conficker worms have in the past.

ESET OFFERS A FREE BLUEKEEP (CVE-2019-0708) DETECTION TOOL TO HELP IDENTIFY SYSTEMS VULNERABLE TO EXPLOITATION VIA RDP. FOR INSTRUCTIONS ON ITS USE AND TO DOWNLOAD A COPY

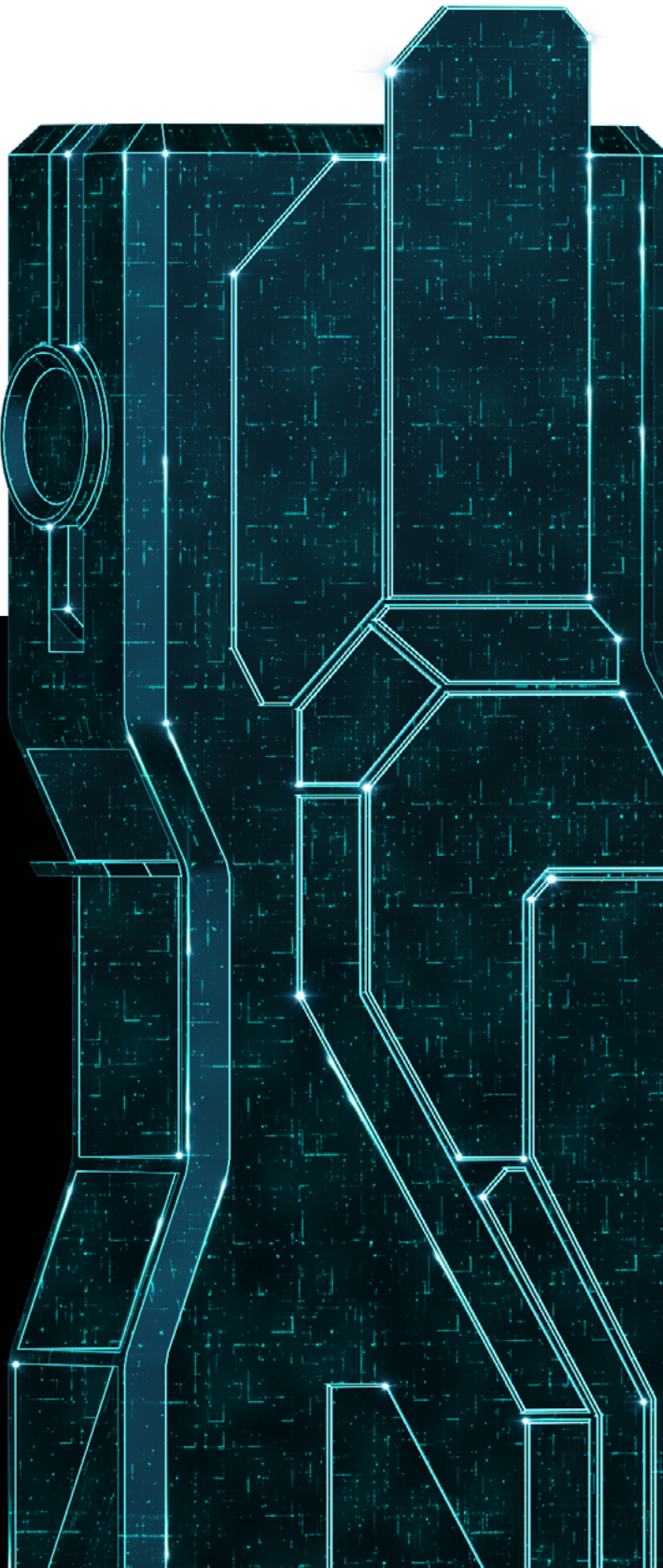
SEE THIS ARTICLE

**Please note:* *Windows 8 and Windows Server 2012 versions and later are reported as unaffected at the time of publishing.*

Exploitation of wormable vulnerabilities is generally considered a severe issue. Microsoft has assigned the vulnerability its highest severity level, Critical, in its published guidance for customers, and in the US government's National Vulnerability Database, the entry for CVE-2019-0708 is scored as 9.8 out of 10. Microsoft issued a blog post strongly recommending that users install its patches, including those for out-of-support operating systems such as Windows XP and Windows Server 2003. Concerns about a wormable exploit were so high that, at the beginning of June 2019, the US National Security Agency issued a rare advisory recommending installation of Microsoft's patches for the flaw.

While making the rounds at various pentesting outfits around the world, no major escalations in BlueKeep activity were reported until November 2019, when mass reports of use of the exploit went public, as noted by ZDNet and WIRED. The attacks were reportedly less than successful, with about 91% of vulnerable computers crashing with a stop error (aka bug check or Blue Screen of Death) when the attacker attempts to exploit the BlueKeep vulnerability. However, on the remaining 9% of vulnerable computers, these attackers successfully installed Monero cryptomining software. While not the feared wormable attack, the criminal group automated exploitation, albeit without a high success rate.

Since time is of the essence let's avoid an overly detailed description of the vulnerability and instead focus on what should be done to protect networks against this threat.



2.

Defending against RDP-borne attackers

So, what can you do? Well, the first thing, is to stop connecting directly to your servers over the internet using RDP or at least minimize this whenever possible. This may be problematic for many businesses, especially now that many employees may be working remotely under various quarantine regimes.

Let us stress, if you are still running Windows Server 2008 or Windows 7 (which are no longer supported as of January 2020) and have machines running these platforms that are directly accessible via RDP, then you are at serious risk of attack and you should take remediation steps immediately. By running these platforms, your threat surface has multiplied by a substantial factor, and the recommendations below should take a back seat to your business updating to platforms that are fully supported by their respective vendors.

For those running up-to-date platforms, the situation does not mean that you have to immediately stop using RDP, but that you need to take additional steps to secure it as soon and as thoroughly as possible. To this end, we have created a table with the Top 12 steps you can take to begin securing your computers from RDP-based attacks.

12 RECOMMENDATIONS FOR SECURING RDP

This table is loosely based on order of importance and ease of implementation, but that can vary depending upon your organization. Some may not be applicable or may be more practical to do in a different order. Your organization may need to take additional steps.

	RECOMMENDATION	REASON
1	Disallow external connections to local machines on port 3389 (TCP / UDP) at the perimeter firewall*	Blocks RDP access from the internet altogether.
2	Test and deploy patches for the CVE-2019-0708 (BlueKeep) vulnerability and enable Network Level Authentication as quickly as possible.	Installing Microsoft's patch and following their prescriptive guidelines helps ensure devices are protected against the BlueKeep vulnerability.
3	For all accounts that can be logged into via RDP, require complex passwords (a long passphrase containing 15+ characters with no phrases related to the business, product names, or users is mandatory).	Protects against password-guessing and credential-stuffing attacks. It is incredibly easy to automate these and increasing password length makes them exponentially more resistant to attacks.
4	To access servers, use unique passwords for local accounts with admin rights (e.g., by using LAPS or a robust password manager service) **Also: Restrict server access rights to a limited group of users.*	*(as above)* Reduces the attack surface of servers by limiting the number of users which can access them.
5	Set the RDP client connection's encryption level to "high," if possible. If not, use the highest encryption level available for connections.	Use 128-bit encryption for all client-server communications, if possible.

6	Install a multi-factor authentication (MFA) solution, such as ESET Secure Authentication (ESA), and require it for all accounts that can be logged into via RDP, as well as for all administrator accounts.	Requires a second layer of authentication only available to employees via mobile phone, token or other mechanism for logging into computers.
7	Install a virtual private network (VPN) gateway to broker all RDP connections from outside your local network.	Prevents RDP connections between the internet and your local network. Allows you to enforce stronger identification and authentication requirements for remote access to computers.
8	Via your security dashboard, assure that your Password-protected endpoint security software is using a strong password unrelated to administrative and service accounts. ESET Security Management Center (ESMC) allows easy, granular policy control and creation of various computer groups. Simultaneously, ESMC allows multitenancy and is accessible by MFA-secured logins.	Provides an additional layer of protection should an attacker gain administrator access to your network.
9	Enable exploitation blocking in endpoint security software, which is a non-signature-based anomaly detection technology that monitors the behavior of commonly-targeted applications.	Many endpoint security programs can also block exploitation techniques. Verify that this functionality is enabled.
10	Isolate any unsecure computer that needs to be accessed from the internet using RDP.	Implement network isolation to block vulnerable computer(s) from the rest of the network.
11	Replace unsecure computers.	If a computer cannot be patched (against the BlueKeep vulnerability), plan for its timely replacement.
12	Consider instituting GeoIP blocking at VPN gateway.	If staff and vendors are in the same country, or among a short list of countries, consider blocking access from excluded countries in order to prevent connections from foreign attackers.

***By default, RDP operates on port 3389**. *If you have changed this port to a different value then that is the port that should be blocked.*

3.

How ESET helps protect your RDP

A good first step is making sure that your endpoint security software is A. up-to-date and B. detects the BlueKeep vulnerability. Then there is a more granular role for layered technology. BlueKeep is detected as RDP / Exploit. CVE-2019-0708 by ESET's Network Attack Protection module, which is an extension of ESET's firewall technology present in ESET's endpoint protection products, version 7 and higher.

Another layer of technology critical to protecting RDP is ESET Exploit Blocker, which monitors typically exploitable applications (browsers, document readers, email clients, Flash, Java, and more. Instead of narrowly aiming only at particular CVE identifiers, it focuses on exploitation techniques. When triggered, the threat is blocked immediately on the machine.

In parallel to technology, we would advise you to put proper processes in place that should be as user-friendly as possible, processes which ultimately benefit from easy to use tools. Since securing RDP requires several (procedural) steps, easy to use multi-factor authentication (MFA) is perhaps most crucial because it acts as a protection against easily-guessed or brute-forced passwords. By focusing on authentication to a system or platform, in this case RDP, you protect one of the most critical systems you have in your business for managing the security of both your network and individual users.

Our MFA solution ESET Secure Authentication (ESA) protects vulnerable communications such as Remote Desktop Protocol by adding multi-factor authentication.

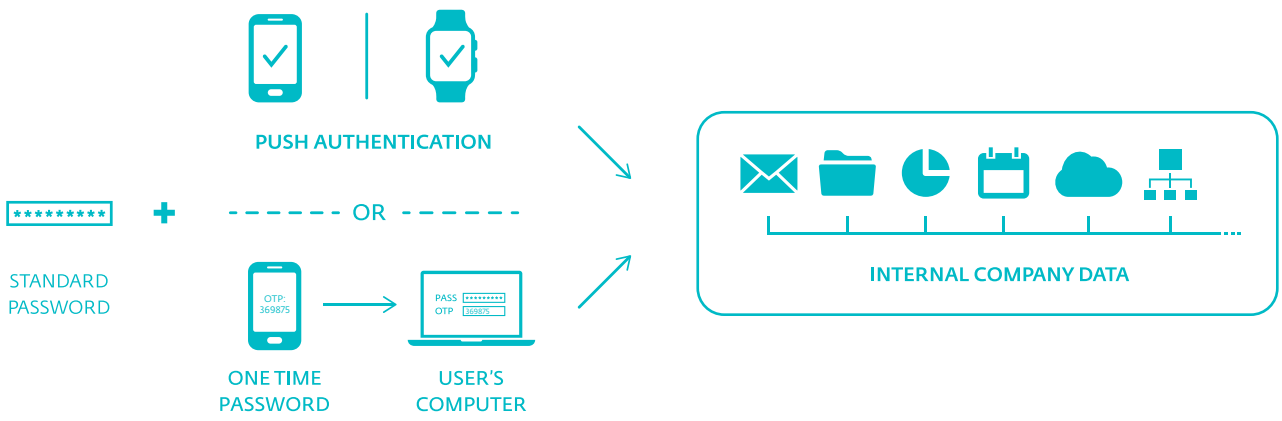
A solution like ESA supports all VPNs (itself a critical safeguard securing access), logins on critical devices that contain sensitive data and cloud services such as Office 365, Google Apps, or Dropbox and many others using ADFS 3.0 or SAML.

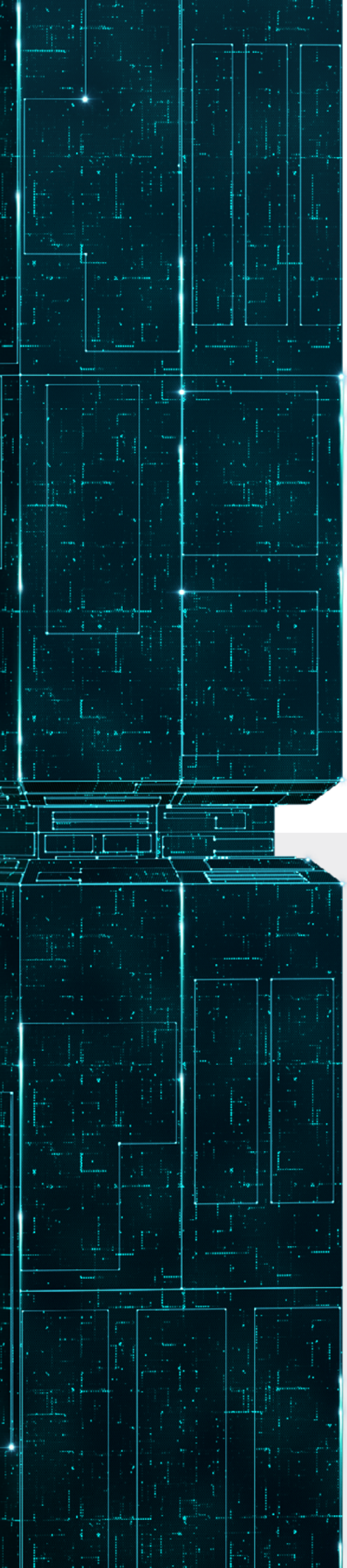
Centrally managed from the browser, ESA was designed to work on all iPhones and Android devices, and also works well with multiple types of authenticators including easy to use push notifications, mobile applications, hardware tokens, FIDO security keys and other custom methods (via the ESA SDK). Parallelly ESA helps secure both company data and the cloud in a simple, yet powerful way, it also helps meet compliance requirements for regulations such as GDPR.

DURING THE COVID-19 PANDEMIC, IN ORDER TO HELP COMPANIES EFFICIENTLY SECURE THEIR CRITICAL SYSTEMS AND PERSONAL DATA, ESET IS EXTENDING THE USUAL ONE MONTH FREE TRIAL OF ESA TO 90 DAYS.

READ ESA SOLUTION OVERVIEW

Lastly, adding full disk encryption as a follow up to MFA is a great step too. ESET Full Disk Encryption (EFDE) provides powerful encryption of system disks, partitions or entire drives. These are managed natively by ESET management consoles ESET Security Management Center and ESET Cloud Administrator, further improving your organization's data security.





KNOWLEDGE IS POWER…FULL SECURITY TOO

Various RDP techniques and tactics can also be examined in the MITRE ATT&CK® knowledge base. While referenced by many vendors' researchers, the ATT&CK KB brings much of this to a shared space. Leveraging ATT&CK and (EDR) tools can be very useful for examining in detail threats facing your network. Tools like the ESET Enterprise Inspector (EEI) allow security admins to examine detections, directly reference the ATT&CK KB for further information and set custom alarms for your network.

Another possibility with RDP borne threats is having (partial) detections, but remaining unprotected. EDR can also play a role in scenarios where clear detections may not occur. For example, in some cases the BlueKeep exploit immediately crashed the targeted system because it proved unreliable. So, in order for the RDP exploit to function it may need to be paired with another exploit, such as an information disclosure vulnerability (for example, via Flash - php files) that reveals kernel memory addresses so that they no longer need to be guessed. This could reduce the likelihood of a crash, as the current exploit performs a large heap spray. These associated behaviors can be flagged with custom rules created within EEI, ultimately triggering an alarm and drawing the admin's attention. Additional network intelligence may also be sourced via regular penetration testing, and checking suspicious behavior via SIEM, IPS, IDS.

CONCLUSION

COVID-19 has changed the way organizations work, not just temporarily throughout the course of the pandemic, but forever. Employers need to adjust not just to the demands of employees working from home now, but in the future as well.

One thing the pandemic has shown us is that many jobs and tasks which formerly were thought of as requiring employees onsite at the office will now be viewed as optimal candidates for remote. But, in order for that to occur, remote workers need to have secure access to the office. ESET offers a variety of solutions that can help businesses provide secure access to corporate resources.