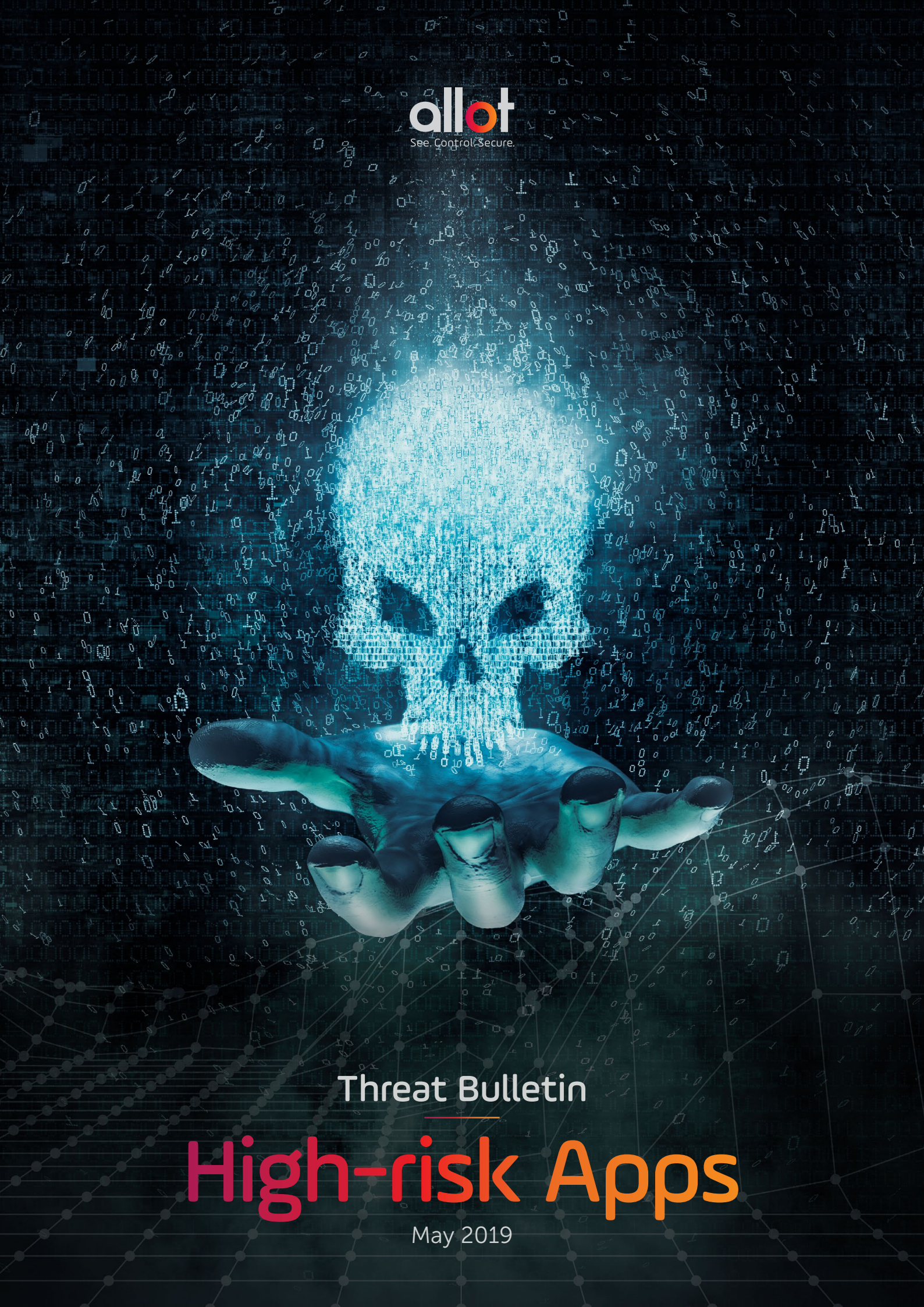


Threat Bulletin

High-risk Apps

May 2019

Intro

Imagine one of your employees decided to download a new episode of his favorite TV show on the corporate network. After finding it on a torrent site, he successfully downloads it without realizing it is bundled with malware. Consequences of torrenting on corporate networks go beyond the legal ramifications of downloading copyrighted material. It raises serious security concerns and can result in a malware outbreak or worse.

The threat is widespread and real. In March 2019, Kaspersky Lab reported an advanced type of malware targeting users of the popular torrent site, The Pirate Bay. The trojan was disguised as a cracked version of legitimate paid software and, due to its multi-layered structure, has been named PirateMatryoshka, after the traditional Russian stacking doll.

Cybercriminals often use torrent trackers for spreading malware disguised as popular software, computer games, media files, or any other hyped content. For example, in April there were a lot of security warnings related to the release of the largely anticipated final season of the popular TV show "Game of Thrones". In 2018, it topped the list of the most common malicious TV torrents that were used by hackers as bait to install malware on people's computers.

Torrent trackers are part of a broader issue organizations face – high-risk applications that can expose the corporate network to multiple security threats.

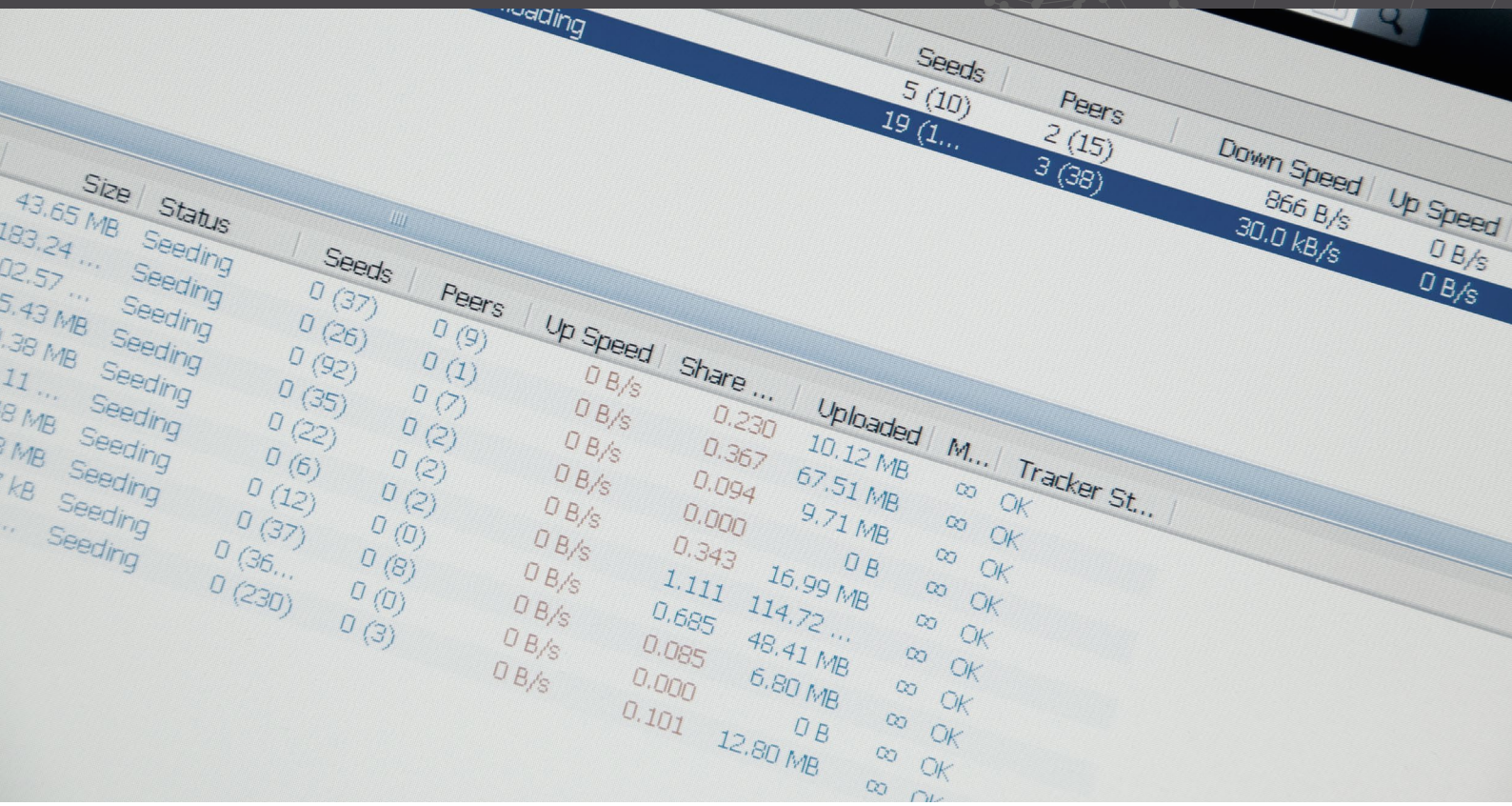
Risk Vectors

Today, an average business uses about 1,181 cloud services. Most of them don't meet recommended security requirements and aren't officially sanctioned by in-house IT departments. Employees are increasingly bringing programs and apps into the workplace without involving IT, with the good intention of streamlining their work and improving productivity. For example, the IT desk of one company was surprised to learn that 600 of their employees were using Dropbox for work files, when Dropbox offered them a business account because of it.

These apps are considered high-risk applications because they may be inherently malicious, but primarily because IT has not evaluated them for their security posture, such as:

- Vulnerabilities that expose them and the corporate network to cyberthreats.
- Robust security access controls, such as two factor authentication and encryption.
- Ownership of the information uploaded to them.
- They may have experienced a data breach.

Many of these applications are often targeted by hackers as they can provide the perfect entry point into the corporate network for malicious activity. Among these apps file sharing, remote admin, torrents and anonymizers are especially risky. Let's look at each of them.



Popular High-Risk Apps

Anonymizers

Examples: Tor, ProxySite.com, HideMyAss, Hide.me, AnonyMouse, Whoer.net, 4everproxy, Dontfilter.us, ProxyTurbo, Megaproxy, Trycatchme.Com, etc.

An anonymizer is a tool that hides a user's real IP address and makes his internet activity untraceable. Anonymizers can be used by employees to bypass corporate restrictions and get access to inappropriate websites, such as hate sites, pornography and gambling sites.

Anonymizers require very little technical skill. Users install a proxy application and configure the web browser to point to a proxy website. After that, when accessing websites, the computer will connect to the proxy server, circumvent the firewall rules, and retrieve blocked websites.

In some cases, employees use anonymizers to conduct personal business on company time and company servers, lowering their productivity and eating up precious bandwidth. Misuse of internet access through anonymizers can expose corporate network to malware and intrusions since they are bypassing IPS and other network-based security systems by design. When installing the program, employees can easily pick up a dangerous virus risking all the company's data and their network.

Torrents (P2P networks)

Examples of torrent clients: BitTorrent, uTorrent, qBittorrent, FileStream.me, BitLord, Vuze, etc.

Examples of torrent sites: ThePirateBay, Torrentz, ExtraTorrent, LimeTorrents, SumoTorrent, Zooqle, 1337X, TorrentDownloads. etc.

In recent years torrenting has gained much popularity with approximately 3.35% of all internet traffic coming from BitTorrent and its 170M+ monthly users. Torrenting allows users to easily download various files such as movies, digital books, songs, software, video games etc. through the torrent client.

Torrenting is a type of peer-to-peer (P2P) file-sharing technology that let users connect and share files with other users around the world without going through a central server. Users install the free client (e.g. uTorrent or BitTorrent) on their computers which enables them to find and download files located on another user's hard drive. These clients also allow files on your hard drive to be shared with other users. If torrent software is not properly configured, users may be unknowingly opening the contents of their entire hard drive to the internet, which can include corporate files never intended for distribution.

Another issue with torrents is that they are often delivered together with malware or adware. A report by BitSight indicates that 39% of the games and 43% of the applications shared via torrent portals are infected with malware. ~25% of companies have employees that sneakily download torrent files, putting their organizations at unnecessary risk. In fact, some worms have been specifically written to be spread by popular peer-to-peer networks – such as PirateMatryoshka, the trojan we mentioned earlier.

Remote Access Apps

Examples: TeamViewer, RemotePC, AnyDesk, Anyplace Control, BeAnywhere, GoToMyPC, LogMeIn, RealVNC, ShowMyPC, SkyFex, etc.

Remote access software lets one computer view or control another computer from anywhere in the world. It's commonly used in enterprises by HelpDesk administrators and other IT support staff, providing remote access to computers within the company for technical troubleshooting.

The access these apps provide may be remote, but the security risks that accompany them are not. For starters, the software is hackable. Hackers often use remote access points to intrude into corporate networks. In fact, in May 2019, Russian hacking group Fxmsp breached three major U.S. anti-virus companies by exploiting internet-connected remote desktop protocol (RDP) and Active Directory servers. The hack went unnoticed as TeamViewer and AnyDesk are both legitimate, and the software was being used by admins in the breached companies. As a result, cybercriminals accessed local corporate networks and stole source codes which they later attempted to sell online.

Remote access vendors regularly report security breaches which is another major security risk accompanying the use of the software these vendors provide. For example, TeamViewer was hacked in 2016, resulting in the penetration of thousands of machines according to reports made by users. Some users even claimed they lost money from their bank accounts.

With remote access to a network, criminals can not only obtain sensitive information and hijack login credentials and identities, they can also deploy ransomware, such as SamSam or Dharma, which can have severe consequences.

Cloud Storage and File Sync Apps

Examples: Dropbox, Google Drive, Microsoft OneDrive, etc.

Cloud storage and file sharing services have seen incredible adoption rates due to their flexibility, scalability, and the savings they provide. Such apps enable companies to back up, synchronize, and store their data in third-party data centers via a cloud provider. However, the security and ownership of corporate data is a key concern for using such apps.

Cloud-based applications allow employees to easily transfer any data out of the organization's IT environment. Employees can easily upload sensitive documents to their personal Dropbox account and this information will stay with them even when they leave the company. This behavior exposes organizations to data leakage, cyberthreats or, in some cases, to different compliance violations (HIPAA, FINRA, SOX, etc.).

Entrusting the control of business data to third-parties includes the inherent risks of enterprise data being accessed or mishandled by the provider. External threats can also lead to data leaks, including hacks of cloud storage providers. Even if a cloud isn't breached, it's possible for hackers to break into individual accounts on Google Drive, Dropbox, Microsoft OneDrive and other platforms. In 2016, more than 68 million Dropbox account credentials were leaked giving cybercriminals a way to intrude into the corporate networks.

Conclusion

The proliferation of cloud-based apps has improved productivity and made information technology significantly more accessible to even novice tech users. Regardless of the intent, the use of unsanctioned applications, shadow IT and/or personal apps are increasing corporate IT risks.

Organizations need to ensure that their corporate network serves the business first and is secured thusly. Risky and malicious applications, including benign applications that are not sanctioned by IT must be blocked as part of this initiative. At the same time, companies need to scan all the traffic allowed into the network for potential threats. To do that, they can use solutions that provide granular network and application visibility and control. By creating and enforcing security policies that can identify, block or limit usage of risky applications, the attack surface is greatly reduced, and security controls are more effective in their operation.