Digital Intelligence
Securing the Future

R&D Security Report

Introduction

Research and development activities occur in many different verticals, with over 1.7% of the UK's GDP in 2019 being spent on R&D[1]. R&D often occurs within specialist divisions of companies, but it can also take place across an entire organisation. Examples of this include "permitted bootlegging" policies. R&D presents an attractive target for Organised Crime Groups (OCGs) looking to profit from extorting, ransoming and selling intellectual property (IP). It is also a target for government-funded Advanced Persistent Threats (APTs) aiming to carry out economic espionage. Notably, R&D has recently been targeted by hacktivists during Russia's invasion of Ukraine.

Supply Chain Security

R&D activities often involve developing custom or evaluating commercial software to see what value it can provide to an organisation. A recent study found that 97% of commercial codebases contained open-source software[2]. Open codebases can allow the community to review and potentially spot vulnerabilities in their code, including those placed by hostile actors. Users will frequently download packages from repositories with absolute trust, believing that as they are hosted on an official website, they must be audited and legitimate. Over 388,000 projects are available on the Python repository pypi alone[3]. This volume means that it is impossible for the community to review every line of code. Packages are often installed through command-line tools, meaning users are unable to complete code reviews before installation.

In 2016, an 11-line NPM package called "left-pad" was unpublished by its author due a naming dispute. When active, it had ten stars on GitHub[4]. This led to high profile packages, such as React and Babel, breaking amid widespread confusion. This is because many people had never heard of left-pad, an obscure dependency. This drives home the risk of complex supply chains. Specifically, malicious code could have been added to left-pad and it is unlikely that users or developers would have immediately noticed.

Unfortunately, the average open-source project has 80 dependencies[5] which makes it difficult or essentially impossible for humans to review all of them. As R&D environments often involve trying new packages and writing new code, staff should be aware of the risk of large dependency trees and be sure to understand what they are installing on their systems.

Users may also accidentally select typosquatted packages. For example, a malicious package called "iconicio" was recently found on NPM imitating the legitimate package "iconic-io"[6]. Malicious packages have been seen to steal credentials, such as Discord tokens and environment variables[7], and act as cryptominers[8].

Even popular and widely contributed to projects, such as the Linux Kernel, are vulnerable to supply chain attacks. In 2021, researchers from the University of Minnesota published a paper showing the feasibility of introducing use-after-free bugs in the Kernel. They slipped them through code review with minor changes that made them look legitimate[9].

Closed source software is also at risk of supply chain attack. Well-known and trusted brands provide an attractive target for attackers. For example, the 2020 attack on SolarWinds Orion[10], attributed to CozyBear, a Russian APT, resulted in the compromise of over 350 organisations, including Intel, Cisco and Microsoft. Attackers used this backdoor to access valuable IP, such as source code[11]. Attackers may also target high-value software, such as in a 2021 when the Passwordstate password manager compromise[12] affected over 29,000 companies.

Physical supply chain security is also an important consideration for R&D environments. Equipment may be manufactured in countries which have active campaigns of economic espionage against R&D groups, introducing a security risk to the supply chain that is exceedingly difficult to manage. Advanced adversaries can intercept and modify hardware, allowing them persistent access to systems. An infamous 2018 Bloomberg article claiming China had placed tiny hardware backdoors on Supermicro servers was disputed by the companies involved[13]. However, a researcher later proved that the alleged hack was technically feasible[14].

Cyjax recently published a White Paper reviewing a supply chain hardening project carried out by a major global organisation[15]. While the report was not specific to R&D, key points from it carry across different sectors. A key takeaway was that a full understanding of the supply chain is difficult, if not impossible to reach. Organisations should find the highest-risk suppliers and focus on them specifically. The hardening project also depended on each supplier having a dedicated contact to provide supply chain data, something that open-source projects are unlikely to have.

Depending on the vertical, R&D activities may require the use of specialised Industrial Control Systems (ICS) equipment. For example, this is needed to coordinate laboratory or manufacturing equipment. ICS systems are frequent targets for both ransomware and cryptominers[16]. Physical security of equipment is also an important consideration. For example, plugging in USB sticks for firmware updates could provide an access route for attackers. Companies should ensure they understand their ICS attack surface, seeking specialist advice when needed.

Data theft and ransomware

R&D departments, by their nature, hold valuable IP that adversaries want to access and either deny or exfiltrate. Compromised data is often ransomed and used for extortion. The double extortion model was first introduced by the Maze ransomware gang at the end of 2019. This model involves threat actors stealing data and demanding two payments, with the first for decryption and the second to avoid the release of data[17].

Double extortion is now a common tactic, adding more pressure on organisations to avoid compromise in the first place. This is because even with backups, they must pay to avoid data leakage. For example, the operators of the Cuba ransomware have been linked to the Industrial Spy marketplace[18]. Some threat actors (TAs) such as Clop and REvil have been seen to contact customers of targeted organisations, asking them to add pressure onto victims to pay[19]. This can cause serious reputational damage to a company, in addition to the damage of losing advanced R&D data.

Ransomware actors have consistently added capabilities to target new platforms. For instance, the Deadbolt ransomware group has recently focused on QNAP NAS devices[20]. TAs are known to adapt their ransomware to commercially popular products, such as Vmware EXSi[21].

The rise of the Ransomware-as-a-Service (RaaS) model adds complexity to the threat landscape. This is where threat actors pay to access ransomware and associated infrastructure but carry out attacks themselves. This can make it harder for analysts to identify a comprehensive list of Tactics, Techniques and Procedures (TTPs) associated with ransomware, as different TAs may use entirely different methods during their operations. For example, ALPHV/BlackCat affiliates have been seen deploying techniques such as exploiting firewalls, VPNs, carrying out RDP bruteforce, and using payloads varying from TeamViewer to Cobalt Strike[22].

As ransomware is common, it also supplies a useful cover for threat actors motivated by data theft or espionage. The BRONZE STARLIGHT threat group, a Chinese-linked APT, has been seen to use ransomware as a red herring for incident responders whilst actually focusing on the theft of data[23].

Some threat actors may also be politically motivated, especially in instances such as during the Russia-Ukraine war. Hacktivists working under the banner of Anonymous have leaked substantial amounts of R&D data from Russian organisations, with an example being from pipeline company Transneft. The IT Army of Ukraine continues to carry out cyberattacks on Russian entities daily. Organisations in pro-Ukrainian countries are also vulnerable to Russian-backed attacks. A recent Microsoft Threat Intelligence Centre (MSTIC) report found that 20% of Russian threat activity outside of Ukraine has been targeted at the IT sector. In a quarter of successful intrusions, MSTIC found successful data exfiltration by the threat actor[24].

Organisations should also consider the risk of insider threats. In a recent joint speech, FBI Director Christopher Wray stated that the Chinese Communist Party (CCP) is “a far more complex and pervasive threat to businesses than even most sophisticated company leaders realize”. The Chinese government

targets R&D across all verticals and companies of all sizes[25]. Notably, they have used insiders during their campaigns to attack R&D divisions. Speaking alongside him, MI5 Director General Ken McCallum highlighted the CCP's manipulation of citizens in the west who are often unaware that they are viewed as "helpful agents of influence" in economic espionage[26]. Non-governmental APTs have also been known to use insiders. For example, Lapsus$ publicly announced in March 2022 that they were seeking to recruit insiders in multiple verticals.

Conclusion

The threat landscape for R&D organisations is varied and fast-changing. Supply chain security is likely to remain a major threat which organisations should try to understand and manage. The fast-moving ransomware landscape is also a serious challenge, as new TAs appear and the number of APTs grows globally. Organisations should ensure they have a comprehensive understanding of their attack surface and use a defence-in-depth security posture to defend their most valuable R&D data. Effective threat intelligence is an important part of successful defence and as such, Cyjax is ready and willing to assist any organisation hoping to understand the landscape.

Emily Dennison
Intelligence Analyst

Endnotes

1 https://www.oecd.org/sti/inno/researchanddevelopmentstatisticsrds.htm
2 https://www.zdnet.com/article/open-source-security-needs-automation-as-usage-climbs-amongst-organisations/
3 https://pypi.org/
4 https://www.theregister.com/2016/03/23/npm_left_pad_chaos/
5 https://snyk.io/reports/open-source-security/
6 https://blog.reversinglabs.com/blog/iconburst-npm-software-supply-chain-attack-grabs-data-from-apps-websites
7 https://jfrog.com/blog/malware-civil-war-malicious-npm-packages-targeting-malware-authors/
8 https://checkmarx.com/blog/cuteboi-detected-preparing-a-large-scale-crypto-mining-campaign-on-npm-users/
9 https://qiushiwu.github.io/papers/OpenSourceInsecurity.pdf
10 https://www.reuters.com/article/uk-usa-cyber-treasury-exclusive/suspected-russian-hackers-spied-on-u-s-treasury-emails-sources-idUKKBN28N0PI
11 https://msrc-blog.microsoft.com/2020/12/31/microsoft-internal-solorigate-investigation-update/
12 https://www.bleepingcomputer.com/news/security/passwordstate-password-manager-hacked-in-supply-chain-attack/
13 https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
14 https://trmm.net/Modchips/
15 https://www.cyjax.com/2022/05/03/lessons-learned-from-supply-chain-hardening-project/
16 https://documents.trendmicro.com/assets/white_papers/wp-2020-report-on-threats-affecting-critical-industrial-end-points.pdf
17 https://www.bleepingcomputer.com/news/security/maze-ransomware-says-computer-type-determines-ransom-amount/
18 https://heimdalsecurity.com/blog/industrial-spy-a-new-stolen-data-market-is-advertised-via-adware-and-cracks/
19 https://krebsonsecurity.com/2021/04/ransom-gangs-emailing-victim-customers-for-leverage/
20 https://www.qnap.com/en/security-advisory/qsa-22-19
21 https://www.bleepingcomputer.com/news/security/linux-version-of-black-basta-ransomware-targets-vmware-esxi-servers/
22 https://www.cyber.gov.au/acsc/view-all-content/advisories/2022-004-acsc-ransomware-profile-alphv-aka-blackcat
23 https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
24 https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/
25 https://www.fbi.gov/news/speeches/directors-remarks-to-business-leaders-in-london-070622
26 https://www.mi5.gov.uk/news/speech-by-mi5-and-fbi

About Cyjax

Cyjax was formed in 2012. Working closely with the financial sector, we developed technologies and methodologies to help stem the advance of digital threats impacting banks and consumers around the world. We quickly established ourselves as a leading provider of cyber threat intelligence capabilities across all industry verticals, a journey we continue today. Cyjax is built on its own growth and remains wholly owned by its founding members in the UK.

Cyjax Limited
The Old Chapel, Union Way
Witney
Oxon OX 6HD

info@cyjax.com
+44 (0)20 7096 0668
www.cyjax.com