CYE Reveals Critical Cybersecurity Flaws of **Online Gaming Giant**

The Challenge:

Conduct a Red Team Exercise to Comply with Regulations

An online gaming giant invested millions of dollars building its cybersecurity program and establishing a robust cybersecurity posture with 24/7 monitoring capabilities. As part of regulatory requirements, the client needed to conduct a red team exercise to evaluate its ability to orchestrate under a real offensive campaign.

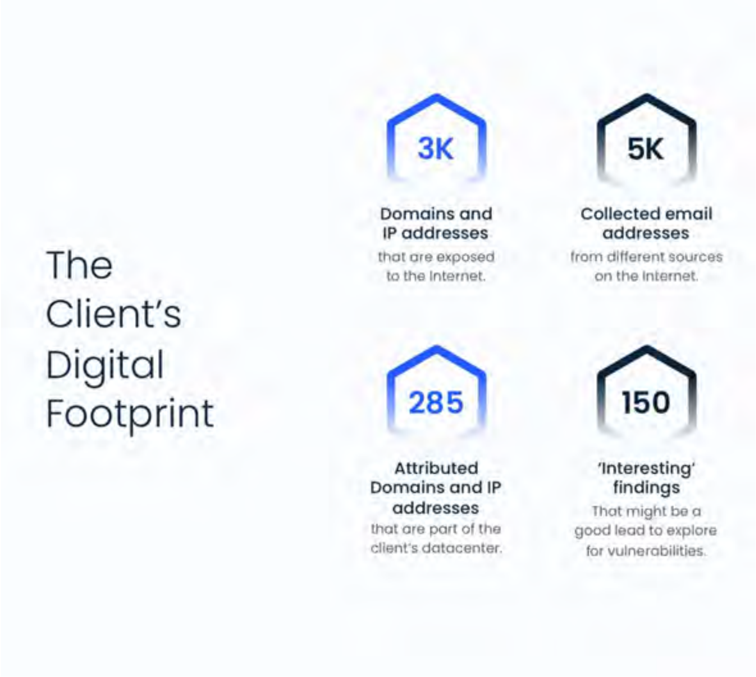
The client chose CYE's red team to attack and identify weak points in the client's new and improved security systems. CYE's team had to assess the client's cybersecurity posture by breaching its internet perimeter, compromising the internal network, and eventually reaching its key business assets. The client then received an optimized mitigation plan with cost-effective recommendations.

CYE operated under black-box conditions, where the client's name was the only information provided. The client had an internal 24/7 SOC that was aware of the assessment and actively looked for CYE's team.

The Solution:

Identify and Exploit Cyber Gaps to Gain Unauthorized Access

Hyver gathered thousands of domains, IP addresses, and email addresses that were exposed to the internet, hundreds of which were attributed to the client's data center and were marked as interesting leads to be further explored for possible exploitation.



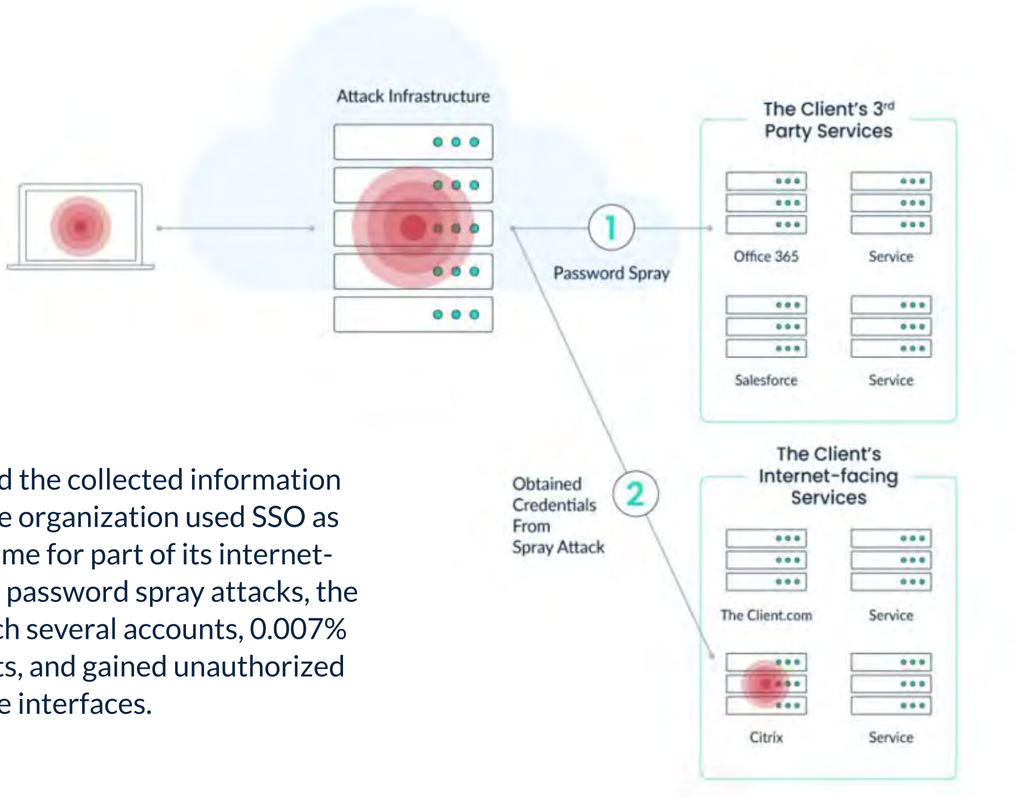
The Client's Digital Footprint

3K
Domains and IP addresses
that are exposed to the internet.

5K
Collected email addresses
from different sources on the internet.

285
Attributed Domains and IP addresses
that are part of the client's datacenter.

150
'Interesting' findings
That might be a good lead to explore for vulnerabilities.

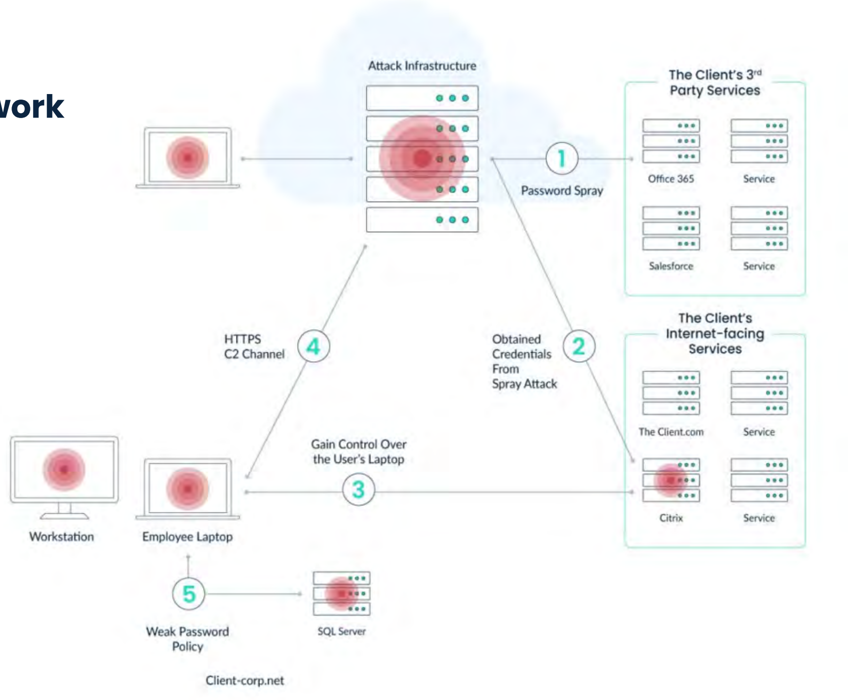

Attack Infrastructure
The Client's 3rd Party Services
Office 365
Service
Salesforce
Service
1
Password Spray
2
Obtained Credentials From Spray Attack
The Client's Internet-facing Services
The Client.com
Service
Citrix
Service

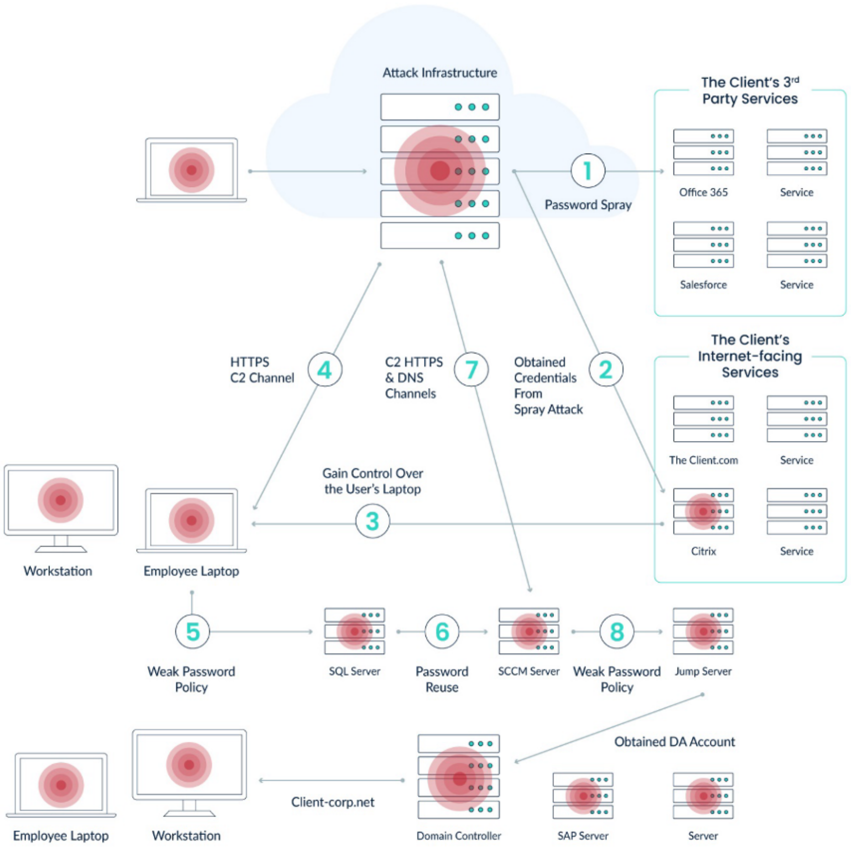
The CYE team analyzed the collected information and discovered that the organization used SSO as an authentication scheme for part of its internet-facing interfaces. With password spray attacks, the team was able to breach several accounts, 0.007% of all collected accounts, and gained unauthorized access to some of those interfaces.

Obtained credentials and lack of MFA made it possible to penetrate the corporate SAP server using a vulnerable Citrix NetScaler interface. Only 0.05% of the exposed IPs and domains needed to be used. Access to sensitive data, even just SAP, could have resulted in severe damage to the organization.

Executing malicious code remotely and establishing a stronger foothold in the network

CYE's team had gained unauthorized but unprivileged access to an interface, which served as the initial foothold to the company's internal network from the internet. The team was able to escape the deployed hardening policy and bypass AV mechanisms to establish persistence in the network. The team was later able to locate and compromise additional assets that were used to escalate the team's privileges in the network.





Compromising the entire domain

The client used a tiered model to separate higher privileged accounts from regular ones. Nonetheless, CYE's team found several weaknesses in the actual implementation and configuration, which enabled unauthorized network access with a local account that was configured with a predictable, widely used password in the organization.

The team gained control over the domain controller, meaning that the entire domain was compromised, yet the attack remained undetected. From a defensive perspective, it is nearly impossible to eliminate the threat, and the attacker can go on to seek sensitive business assets. CYE's team was able to extract financial data (including users' bank accounts and credit card numbers), PII, licenses, sensitive code, and so on—all of which have the potential to cause major financial and reputational damage.

> **"We thought we had confidence in our cybersecurity program before the assessment, but we surely did not expect these results. What started as a semi-bureaucratic regulatory requirement ended up being one of the most important security projects we've had in the past few years."**
>
> Global CISO of "the client"

The Impact:

Stronger Cybersecurity Maturity and Resilience

All assessment goals were achieved. CYE's team gained access to business assets including players' data, billing information, licenses, CRM, and sensitive information of C-level executives.

CYE's team worked together with the client to build an optimized mitigation plan that would significantly reduce the chances of real potential cyber threats. Hyver's business risk evaluation capabilities provided a cost-effective prioritization of mitigation projects by analyzing severity, exploitability, business impact, and mitigation costs and efforts. CYE's team supported the client's team in mitigating the vulnerabilities with expert recommendations, guidance, and verification.

Within a few months, the client improved its cybersecurity maturity score across all main domains and thus strengthened its cyber resilience.

> **"One of the biggest challenges in the gaming industry is that companies focus too much on the 'front gates' but neglect other zones in the attack surface that put business assets at risk."**
>
> Reuven Aronashvili, CEO of CYE

About CYE

CYE's optimized cyber risk quantification platform and expert guidance transform the way organizations manage cybersecurity. Using AI, machine learning, and innovative technology, CYE visualizes attack routes, quantifies, mitigates, and communicates cyber risk, and matures organizational cybersecurity posture. In doing so, CYE provides clear and relevant insights that empower companies to make effective cybersecurity decisions. The company serves organizations in multiple industries globally. Founded in 2012, with headquarters in Israel and operations around the world, CYE is funded by EQT Private Equity and 83North. Visit us at cyesec.com.

CYE