CYE | Customer case study

Online Casino Giant Fact-Checks Its Premium Security with CYE

A heavily guarded online gaming company tested its security posture with CYE's Hyver and red-team experts, revealing major security gaps.

Industry

Gaming

The customer

Global leading online casino

Revenue	Employees	Daily users
$400M	1.1K	13M

CYE solutions

Cybersecurity Assessment and Security Maturity Program

The challenge

The Client invested millions of dollars in 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 solution

CYE's team was tasked 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.

The results

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. The Client implemented Hyver's mitigation recommendations and increased its security maturity score and 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

The background

Looking to adhere to regulatory requirements and having invested significant amounts of money in their cybersecurity program, the Client chose CYE's red team to attack and identify any weak points in their new and improved security systems. CYE operated under black-box conditions, where the only info that was provided by the organization was its name. The Client had an internal 24/7 SOC that was aware of the assessment and was actively looking for CYE's team.

Setting the groundwork for the offensive assessment

The Client's Digital Footprint

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

13K
Collected email addresses
from different sources on the Internet.

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

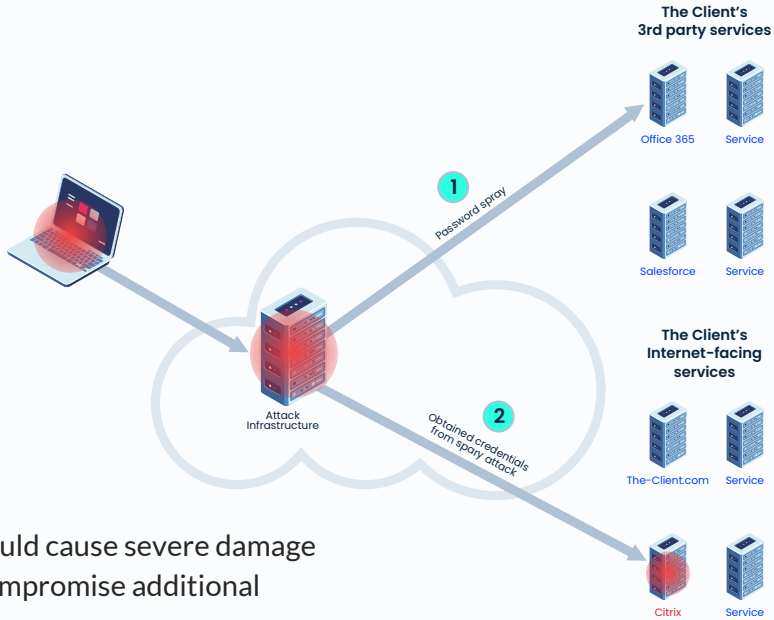
150
'Interesting' findings
That might be a good lead to explore for vulnerabilities.

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.

Using a fraction of the collected data to gain initial access

The CYE team analyzed the collected information and discovered that the organization uses 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.

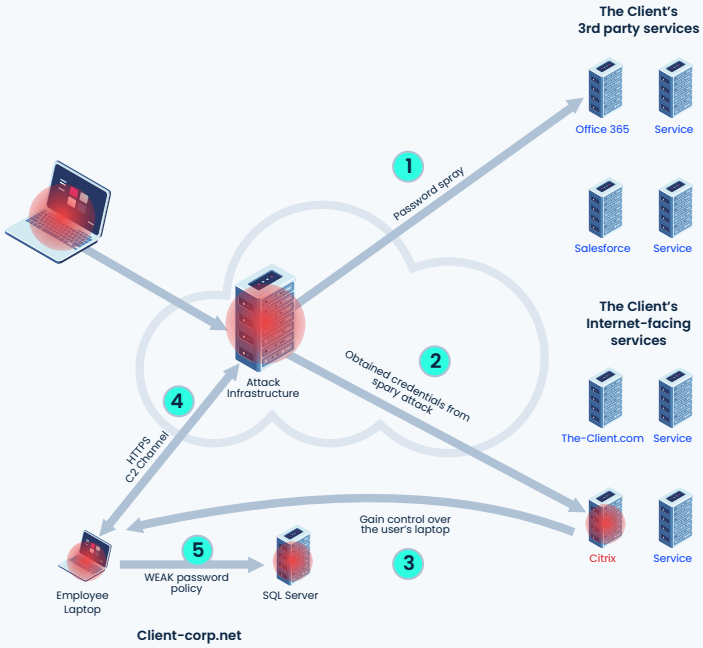
Obtained credentials and lack of MFA made it possible to penetrate the corporate SAP server using a vulnerable Citrix NetScaler interface. Only 0.05% of the exposed IPs and domains were needed to be used.



Access to sensitive data, such as SAP, by itself, could cause severe damage to an organization. The team had continued to compromise additional internal assets.

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

The team had gained unauthorized but unprivileged access to an interface, which served as the initial foothold to the company's internal network form the Internet. The team was able escape the deployed hardening policy and bypass AV mechanisms to establish a 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.

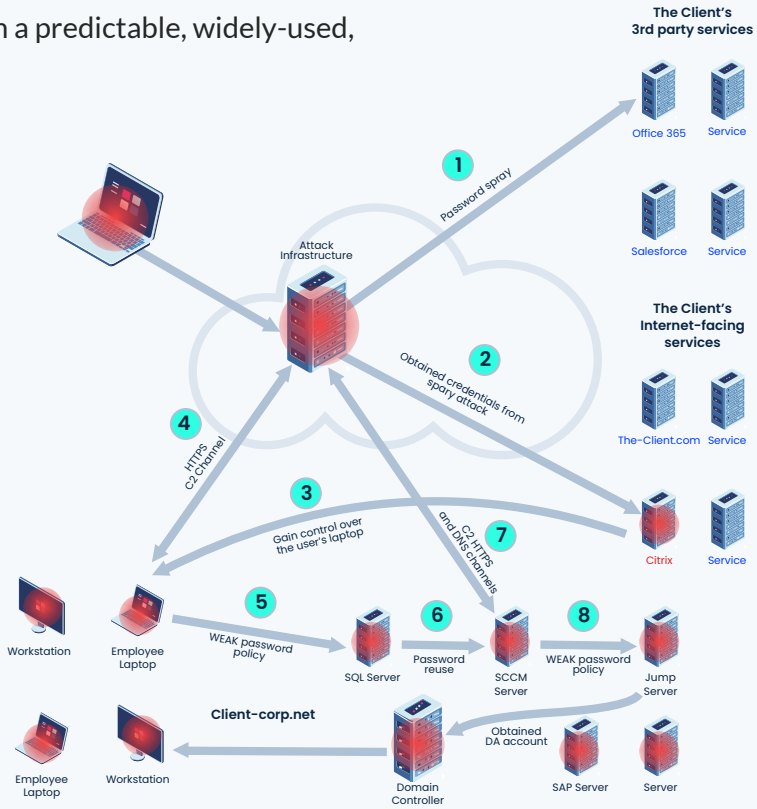


Hyver gathered thousands of domains, IP addresses and email addresses that were exposed to the Internet, hundreds of which were attributed to the Client's data center and were marked as interesting leads to be further explored for possible exploitation.

Compromising the entire domain

The Client used a tier model to separate higher privileged accounts from regular ones. Nonetheless, CYE's team had 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 – the entire domain was now compromised and 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 in a position to extract financial data (including users' bank accounts and credit card numbers), PPI, licences, sensitive code, and so on -- all of which have the potential to cause major financial and reputational damages.



Breaking down to build up

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 allowed a cost-effective prioritization of mitigation projects by analyzing severity, exploitability, business impact, and mitigation costs & 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 thereby increased its cyber resilience.

> " 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"

The Global CISO at "the Client"

About CYE

Founded: **2012**
Offices: **Israel, US, Europe**
300+ global customers

CYE is a trusted advisor to medium-sized and Fortune 500 companies in multiple industries around the world, bringing a fact-based approach to organizational cyber-defense, while managing real business risks and optimizing the cybersecurity investment.

To learn more about our solutions, visit www.cyesec.com

CYE