

Kevin Borgo **Tobias Fiebic** Shuang Hao Christopher Giovanni Vig

CLOUD STRIFE Mitigating the Security Risks of **Domain-Validated Certificates**

kevinbo@cs.ucsb.edu
t.fiebig@tudelft.nl
shao@utdallas.edu
chris@cs.ucsb.edu
vigna@cs.ucsb.edu

Applied Networking Research Workshop (ANRW 2018) / IETF 102







Arne Swinnen (arneswinnen)		4002 76t Reputation Rank	h 6.81 97th Signal Percentile
129 #219205 t	Authentication bypass on auth.uakeover of saostatic.uber.com	ıber.com via subdon	nain Share:
State	Resolved (Closed)	Severity	Critical (9.3)
Disclosed publicly	July 12, 2017 5:43pm -0700	Participants	
Reported To	Uber	Visibility	Public (Full)
Weakness	Improper Authentication - Generic		
Bounty	\$5,000		

STALE DNS RECORDS AND IP ADDRESS RE-USE

cloudstrife.seclab.cs.ucsb.edu

- How to migrate DNS gracefully?
- When to release 34.215.255.68? TTL? Longer?
- What about failure and automatic scaling?

Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates (ANRW 2018)

▶ 34.215.255.68



DOMAIN-VALIDATED CERTIFICATES

- Standard TLS certificate
- Trusted by major browsers and operating systems
- Credited for the rise in HTTPS adoption
- Cheap or free
- No identity verification



Let's Encrypt Hits 50 Million Active **Certificates and Counting**

BY GENNIE GEBHART AND SETH SCHOEN | FEBRUARY 14, 2018

Kevin Borgolte

Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates (ANRW 2018)



via https://nettrack.info/ssl certificate issuers.html



HTTP-BASED DOMAIN-VALIDATION



If you control the host behind the domain, then you can prove domain ownership successfully.

Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates (ANRW 2018)

Kevin Borgolte





- Trusted TLS certificates (MitM)
- Malicious and remote code loading
- Subdomain attacks
- Email (no MX = A record)
- Spam & phishing (residual trust)

Feb 5, 2018 - James Ritchey 😽

GitLab Pages Security Issue Notification

Issue Summary

Kevin Borgolte

When a user adds a custom domain to their Pages site, no validation was being performed to ensure the domain was owned by that user. This issue allows an attacker to discover DNS records already pointing to the GitLab Page IP address which haven't been claimed and potentially hijack them. This issue impacts all users who have created and then deleted custom domains using GitLab Pages, but still have the DNS records active.

Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates (ANRW 2018)

Comodo SSL > Wildcard SSL Certificate

Wildcard SSL Certificate

- Best combination of flexibility, compatibility, and value -

- Get Comodo SSL if you want:
- Multiple subdomains $\overline{\mathbf{M}}$
- Multiple servers \mathbf{M}
- Fast online validation

1 Yr: \$449.95 /yr 2 Yrs: \$427.95 /yr - save 5% ✓ 3 Yrs: \$404.95 /yr - save 10%

ADD TO CART

Arne Swinnen	(arneswinnen)	4002 Reputation	76th Rank	1 6.81 Signal	97th Percentile
A 129 #219205 ta	Authentication bypass on auth.ube akeover of saostatic.uber.com	er.com via suk	odom	nain	Share:
State	Resolved (Closed)	Sev	verity	Critical (9.3)
Disclosed publicly	July 12, 2017 5:43pm -0700	Partici	oants		J
Reported To	Uber	Vis	ibility	Public (Full)	
Weakness	Improper Authentication - Generic				
Bounty	\$5,000				





- How many active domains point to free IPs?
- Looking at cloud IP address (AWS, Azure)
- 1.6 million unique IPs, 14 million allocations
- 130 million unique domains
- >700,000 domains can be taken over within minutes by attacker



- Assume takeovers can and will happen in the future
- Major changes to DNS or deployment impractical
- Aim to prevent attacks higher up
- Focus on TLS services
- Leverage existing standards when possible

Kevin Borgolte

Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates (ANRW 2018)



MITIGATING TAKEOVER ATTACKS

- HTTP, simple idea:

 - HTTPS with trusted certificates domain-validated certificates HTTP Strict Transport Security
 - HTTP Public Key Pinning deprecated since Chrome 67

Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates (ANRW 2018)



- Takeover attacks now require pinned certificate. Reduces takeover attacks to denial of service attacks.
 - Doesn't work for SMTP etc. though



MITIGATING TAKEOVER ATTACKS

- HTTP, better idea:
 - HTTPS with trusted certificates
 - Prevent certificate issuance for domains (likely) taken over
 - HTTP Strict Transport Security

Kevin Borgolte

Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates (ANRW 2018)



No trusted certificate = also works for SMTP etc. How do you prevent certificate issuance?



10

CERTIFICATE TRANSPARENCY LOGS

- Public append-only log for issued certificates
- Monitor for suspicious certificates
- Real-time(ish) audit trail

In itself:

- Reactive: attacker's window of opportunity remains
- Must be actively monitored (by domain owners)

Can be used for historic lookups

11

PREVENTIVE HTTP-BASED DOMAIN-VALIDATION



Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates (ANRW 2018)

12

- Prevents TLS certificates to be issued for takeovers No certificate = takeover attacks less useful (= DoS)
- Drawbacks for users only for disaster recovery
 - Re-bootstrap chain of trust
- ACME validation challenge draft next?



Thank you! **Questions?**





THE COMPUTER SECURITY GROUP AT UC SANTA BARBARA

kevinbo@cs.ucsb.edu https://kevin.borgolte.me twitter: @caovc

