Phishing URL reported **June 24**

http://aaronsse.info/gatech/

Dangerous | aaronsse.info/gatech/

Georgia Tech

Georgia Tech Login Service

Enter your GT Account and Password

GT Account:
Password:
Warn me before logging me into other sites.
LOGIN CLEAR

ATTENTION: When you are finished using all of your authenticated applications, please log out of this system and exit your browser to ensure you do not leave any of your applications (such as your e-mail) open to other users of this machine.

TERMS OF USE
This computer system is the property of the Georgia Institute of Technology. Any user of this system must comply with all Institute and Board of Regents policies, including the Acceptable Use Policy, Cyber Security Policy and Data Privacy Policy (http://b.gatech.edu/it-policies). Users should have no expectation of privacy, as any and all files on this system may be intercepted, monitored, recorded, copied, inspected, and/or disclosed to authorized personnel in order to meet Institute obligations.
By using this system, I acknowledge and consent to these terms.

I don't know my GT Account

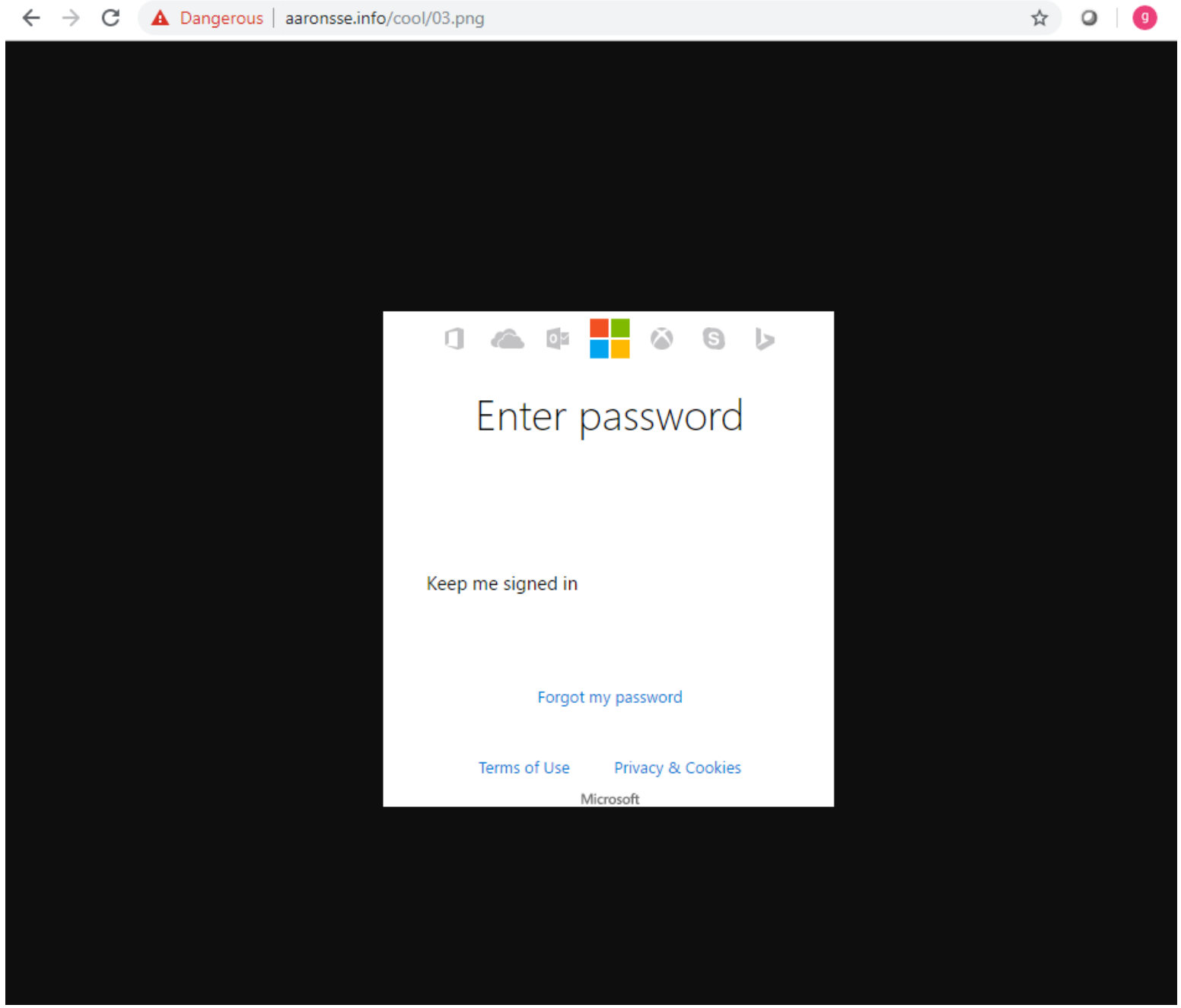
I don't know my password

My correct username and password aren't working

For assistance, please contact the OIT Technology Support Center at 404-894-7173 (Mon-Fri 8am-5:00pm ET).

Additional documentation including how to integrate your application with GT Login

- Emergency Information
- Legal & Privacy Information
- Accessibility
- Accountability
- Accreditation
- Employment


Dangerous | aaronsse.info/cool/03.png
Enter password
Keep me signed in
Forgot my password
Terms of Use
Privacy & Cookies
Microsoft

Domain Name: AARONSSE.INFO
Registry Domain ID: D503300001049604980-LRMS
Registrar WHOIS Server: whois.ovh.com
Registrar URL: http://www.ovh.com/
Updated Date: 2019-07-09 T00:14:20Z
Creation Date: 2019-06-17 T22:21:34Z ← domain created a week before the phishing
Registry Expiry Date: 2020-06-17 T22:21:34Z
Registrar: OVH sas
Registrar IANA ID: 433
Registrar Abuse Contact Email: email@ovh.net Registrar Abuse Contact Phone: +33.972101007
Reseller:
Domain Status: OK
Registrant Organization:
Registrant State/Province:
Registrant Country: DZ
Name Server: NS2.POSITIVEBENEFITS.CO.UK ← hosting for a hypnotherapist, registered in 2011
Name Server: NS1.POSITIVEBENEFITS.CO.UK
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form is https://www.icann.org/wicf/

Where’s the domain hosted? DNS query:

;QUESTION

AARONSSE.INFO. IN A

;ANSWER

AARONSSE.INFO. 14399 IN A 139.99.73.130

;AUTHORITY

;ADDITIONAL

Where's that IP address?

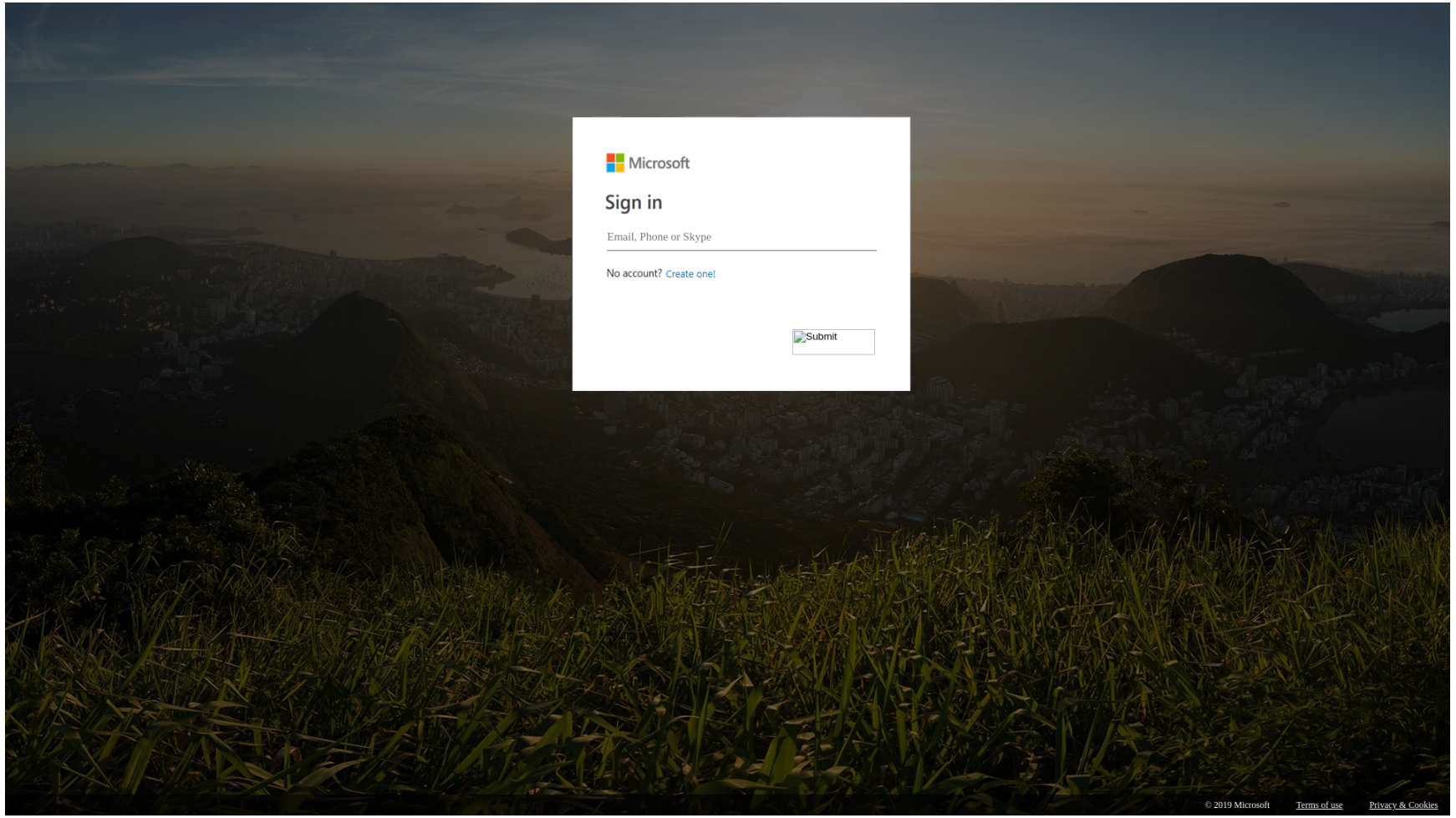
OrgName: OVH Singapore PTE. LTD
OrgId: OSPL-8
Address: 135 Cecil Street #10-01 Myp Plaza
City: SINGAPORE
StateProv:
PostalCode: 069536
Country: SG
RegDate: 2016-09-15
Updated: 2016-09-15

What other domains were on that IP address?

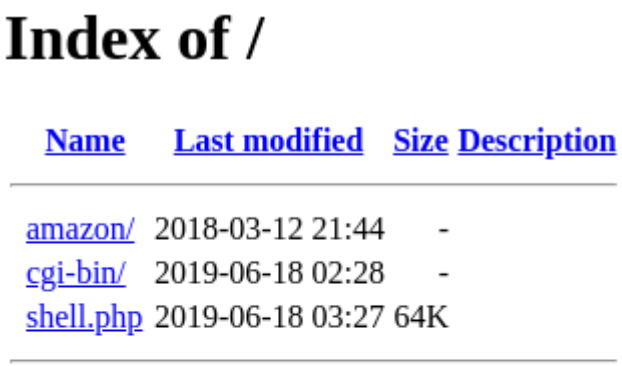
aaronsse.com, aaronsse.info, aaronsse.org, jamessene.com, jamessene.info, jamessene.org, jertivsxzsc.com, kimalemees.com, kimalemees.info, kimalemees.org, kinneynneb.com, kinneynneb.info, michaelooles.com, michaelooles.info, michaelooles.org, mtzasxdwn.com, parrllekr.com, parrllekr.info, parrllekr.org, service-mtzasxdwn.com, sheltonse.com, sheltonse.org, shinolesse.com, shinolesse.info, shinolesse.org, spencerettes.com, spencerettes.info, spencerettes.org, sttonssege.info, sttonssege.org

Which are registered by the same party? Which are maliciously registered? Over-block or under-block?

Phishing on those domains had been taking place for several days before the Georgia Tech phish. For example, June 20: www.outlook.jamessene.com



And June 18: phishing on sheltonse.com



Index of /

Name	Last modified	Size	Description
amazon/	2018-03-12 21:44	-	
cgi-bin/	2019-06-18 02:28	-	
shell.php	2019-06-18 03:27	64K	

- Goal is to respond appropriately, effectively, and proportionately, to prevent victimization
- Data minimization is possible
- Alternatives not as effective
- GDPR Recital 49 says that such is legitimate.