Diving Deep into UNC1151's Infrastructure: Ghostwriter and beyond

prevailion.com/diving-deep-into-unc1151s-infrastructure-ghostwriter-and-beyond/

September 1, 2021

1 September 2021

Introduction:

Prevailion's Adversarial Counterintelligence Team (PACT) is using advanced infrastructure hunting techniques and Prevailion's unparalleled visibility into threat actor infrastructure creation to uncover previously unknown domains associated with UNC1151 and the "Ghostwriter" influence campaign. UNC1151 is likely a state-backed threat actor [1] waging an ongoing and far-reaching influence campaign that has targeted numerous countries across Europe. Their operations typically display messaging in general alignment with the security interests of the Russian Federation; their hallmarks include anti-NATO messaging, intimate knowledge of regional culture and politics, and strategic influence operations (such as hack-and-leak operations used in conjunction with fabricated messaging and/or forged documents). PACT assesses with varying degrees of confidence that there are 81 additional, unreported domains clustered with the activity that FireEye and ThreatConnect detailed in their respective reports [1,2,4]. PACT also assesses with High Confidence that UNC1151 has targeted additional European entities outside of the Baltics, Poland, Ukraine and Germany, for which no previous public reporting exists.

Situation Overview:

In July of 2020, FireEye's Mandiant released a threat intelligence report [1] on an influence campaign they dubbed "Ghostwriter," wherein they detailed a cluster of activity that demonstrated an "anti-NATO agenda" that "primarily targeted audiences in Lithuania, Latvia,

and Poland with narratives critical of the North Atlantic Treaty Organization's (NATO) presence in Eastern Europe." In April of 2021, ThreatConnect published a Threat Intel Update [2] that included possible related Ghostwriter infrastructure spoofing military organizations in Poland and Ukraine, and quotes German investigative reporting [4] detailing Ghostwriter activity against members of the German government and claiming a possible connection to the Russian state. Later in April of 2021, Mandiant released an update to their initial report [3], wherein they attributed at least some of the Ghostwriter activity to UNC1151, "a suspected state-sponsored cyber espionage actor that engages in credential harvesting and malware campaigns." In May of 2021 (the following month), DomainTools released a report consisting of UNC1151 infrastructure [5] that corroborated previous findings and included previously unreported infrastructure and network-based IOCs related to UNC1151. Finally, in August of 2021, VSQUARE released an exhaustive analysis [6] of the Ghostwriter influence campaign that corroborated previous findings linking Ghostwriter/UNC1151 activity to the Kremlin and detailing the group's activity back to 2017 (and possibly earlier), during which time the group was identified using its phishing infrastructure to send targeted spearphishing messages and engaging in politically-destructive hack-and-leak operations.

It may assist the reader to detail a brief timeline of notable events of interest that were reliably reported and attributed [6]:

- *in 2014, attempts to gain access to the Polish Ministry of National Defence using the phishing domain `poczta.mon.q0v[.]pl` (later attributed to APT28).*
- *in 2016, similar attempts were made leveraging a phishing domain displaying a similar pattern: `poczta.mon-gov[.]pl`. The systems of the United States Democratic National Committee were breached by APT28 (Fancy Bear) and APT29 (Cozy Bear), likely operating independently. This access led to an infamous hack-and-leak operation to damage the presidential campaign of Hillary Clinton.*
- *in 2017, from March onward, an unidentified group was observed waging a European disinformation campaign dubbed "Ghostwriter" by FireEye.*
- *in 2018, UNC1151 registers phishing domains, among them `poczta.mon-gov[.]ml` "with the clear intention of stealing data from the address employees used to log into their email." The Lithuanian CERT also publishes a report on an attack later attributed to Ghostwriter [3].*
- *in 2019, the Lithuanian CERT publishes another [3] report on an attack later attributed to Ghostwriter.*
- *in 2020 phishing domains were registered and structured in order to spoof poczta.ron.mil.pl, used by "employees of Poland's Ministry of National Defence working remotely." [6]. Additional phishing infrastructure is registered. Attackers gain access to the personal email of the chief of the Chancellery of the Prime Minister of Poland. Various influence operations take place in Poland.*

- *in 2021, UNC1151 was identified targeting the login credentials of German politicians [3]. Influence operations continue, but now inauthentic messaging is being spread from hijacked accounts as well as fake personas. Influence operations take place in Lithuania [6]. As a result of domestic strife, a well-known Belarusian opposition blogger's flight is hijacked while en route to Lithuania and imprisoned. Previously observed phishing and influence operations continue into the summer.*

PACT identified overlapping TTPs throughout this investigation, notably the techniques used to carry out influence operations (e.g., phishing for credentials to engage in hack-and-leak) and domain and subdomain naming themes such as `poczta` and other Polish and Ukrainian words. Previous reports [6] have attributed these overlaps in behavior displayed by distinct groups (APT28, APT29, and UNC1151) to hypothesize that all this activity is related in some way to the Russian state generally and its intelligence apparatus specifically; PACT agrees with this assessment: it is likely that UNC1151's activity is either controlled or influenced by Russian intelligence services. PACT is not attributing the activity of APT28 and APT29 to UNC1151 or vice versa.

Actor Overview:

UNC1151 and the associated Ghostwriter campaign are broad in both scope and target; previous reporting indicates targeting of audiences within the Baltic nations (Estonia, Latvia, and Lithuania) as well as Germany, Poland, and Ukraine. Analysis of phishing infrastructure from these reports indicates the group was targeting official government accounts (both civil and military) as well as personal accounts. Additional analysis by PACT indicates the targeting of yet other audiences.

Previous reporting and additional analysis suggest that one of UNC1151's behaviors is to use root domains with common, seemingly-legitimate words and themes (e.g., `net-account[.]online` or `login-telekom[.]online`) and then build upon them with specific, targeted subdomains to create long URLs that make their phishing domains look legitimate (e.g., `gmx.net-account.online` or `verify.login-telekom[.]online`). Additional examples appear elsewhere in this report and demonstrate UNC1151's ability to craft convincing domains that allow them to capture credentials in highly-targeted spearphishing campaigns that can then be used for follow-on influence operations: hack-and-leak and inauthentic messaging (sending forged or manipulated messages or posting inflammatory material from hijacked or fake accounts). This ability, combined with UNC1151's reported capacity to understand and exploit pre-existing socio-cultural fissures to sow discord and angst in the targeted states (in accordance with Moscow's security goals) can prove damaging and difficult to counteract, and therefore should be underscored.

PACT identified domain and subdomain naming themes that indicated targeting of the following audiences: Ukrainian and Polish government (particularly the defense sector) (image 1,2), European iPhone and iCloud users (image 3), the French Defense Information and Communication Delegation (DICoD) (a department of the French Ministry of the Armed

Forces) (image 4), and users of popular regional web service providers across Europe and Russia (images 5-8), as well as global tech giants like Google, Microsoft, Apple, Twitter, and Facebook (images 9,10).

Image 1: Phishing domain crafted to target Ukrainian government accounts.

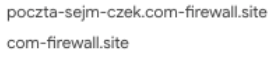

Image 2: Phishing domain crafted to target Polish government accounts.

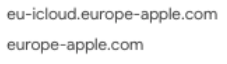

Image 3: Phishing domain crafted to target European iCloud users.

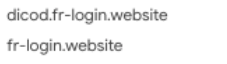

Image 4: Phishing domain crafted to target French DICoD accounts.

Image 5: Phishing domain crafted to target meta.ua, a popular Ukrainian web services provider.

Image 6: Phishing domain crafted to target bigmir) net, a large information and entertainment portal based in Ukraine.

Image 7: Phishing domain crafted to target “interia.pl”, a large Polish web services provider.

Image 8: Phishing domain crafted to target “ukr.net”, a Ukrainian web services portal.

Image 9: Phishing domain crafted to target Twitter accounts.

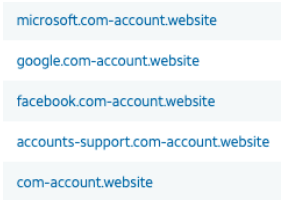

Image 10: Phishing domain crafted to target accounts of major social media and tech giants.

UNC1151 has proven the effectiveness of these tactics, as hundreds of victims, including members of the Polish Parliamentary Intelligence Committee and the chief of the Chancellery of the Prime Minister of Poland, took the bait and gave attackers access to their private email accounts [6]. Unfortunately, the successful phishing of its targets is only an initial, enabling feature of UNC1151’s operational methodology. The actor then uses that access for follow-on influence operations.

Investigative Methodology

PACT leveraged Prevailion's unique visibility and proprietary intelligence platform, along with previous public reporting, to identify patterns and cross-reference web infrastructure (e.g., historical domain registration, TLS certificate, DNS, and hosting data) to aid in the identification of additional UNC1151 infrastructure. PACT identified an additional 83 domains associated with UNC1151 that have not been previously reported: 52 of which PACT assesses with High Confidence *are* or *were* part of UNC1151's operational infrastructure, and 31 that PACT assesses with Moderate Confidence to be previously-used phishing infrastructure for the actor's targeted phishing campaigns.

The High Confidence cluster has been cross-referenced with previous public reporting and is listed at the bottom of this blog; PACT also included the rest of the UNC1151 infrastructure from previous reporting for defenders' and researchers' convenience. This cluster includes the phishing domains that PACT assesses with high confidence were intended to gain login credentials for members of the French Defense Ministry's DICoD. Much of this cluster appears designed to capture login credentials for official and personal accounts of Polish and Ukrainian audiences (images 11,12); common subdomain themes are shared throughout (images 13-16). Activity related to this cluster of domains is ongoing, as evidenced by the registration of `login-inbox[.]site` on 2021-08-20.

poczta.ron-mil-pl.space
ron-mil-pl.space

Image 11: Phishing domain crafted to target official accounts of a Polish audience.

webmail.meta-ua.online
meta-ua.online

Image 12: Phishing domain crafted to target personal accounts of a Ukrainian audience.

poczta.wp-pl.space
wp-pl.space

poczta.wp-pl.online
wp-pl.online

poczta.wp-pl.site
wp-pl.site

poczta.interia-pl.online
interia-pl.online

Image 13-16: Phishing domains displaying common subdomain themes.

The Moderate Confidence cluster was identified using observed hosting commonalities, previous reporting on widespread phishing campaigns [6], and commonalities of domain and subdomain naming themes [2]. This cluster of activity was active as recently as July 2021, but most of the domain registrations occurred in 2019 with expirations in 2020. The naming themes indicate a targeted audience of Apple (iPhone and iCloud) users in Europe; nearly all root domains have at least one subdomain that includes the words "apple" or "icloud"

(images 17,18). Additional subdomains appear to target Paypal and OVH Telecom logins as well (images 19,20). If PACT is correct in attributing this activity to UNC1151, this cluster of mostly-expired Moderate Confidence activity indicates a change in targeting around 2020/2021, as Ghostwriter was primarily aimed at an audience in Poland, Ukraine, and the Baltics (as one can easily see with a quick glance at the subdomains in the High Confidence cluster). This Moderate Confidence cluster, by contrast, appears to have explicitly targeted European iCloud users.

icloud.com-site.in com-site.in	Image 17: Phishing domain crafted to target Apple/iCloud accounts.
apple.com.idlog.in idlog.in	Image 18: Phishing domain crafted to target Apple/iCloud accounts.
paypal.com-ids.info com-ids.info	Image 19: Phishing domain crafted to target Paypal users.
ovhtelecom.com-id.info com-id.info	Image 20: Phishing domain crafted to target OVH Telecom.

Conclusion

PACT is unable to verify that UNC1151 is a homogenous group with central direction; PACT also cannot verify that all Ghostwriter activities were conducted by UNC1151, as PACT analysts only have visibility into the web-based infrastructure. It is possible that phishing infrastructure creation, credential gathering, access, and the influence operations were centrally directed or controlled but carried out by different groups. It is clear, however, that there is an overarching theme and direction to these activities. It is this theme and direction that PACT has identified and continues to track under the UNC1151 actor, which corroborates the reports cited below.

PACT continues to track UNC1151 and the Ghostwriter campaign by leveraging Prevailion's unique and unparalleled visibility into malicious infrastructure creation, and will publish follow-on updates as they are identified and corroborated.

References

[1] https://www.fireeye.com/blog/threat-research/2020/07/ghostwriter-influence-campaign.html

[2] https://threatconnect.com/blog/threatconnect-research-roundup-threat-intel-update-april-1st-2021/

[3] https://www.fireeye.com/blog/threat-research/2021/04/espionage-group-unc1151-likely-conducts-ghostwriter-influence-activity.html

[4] https://www.tagesschau.de/investigativ/wdr/hackerangriffe-105.html

[5] https://www.domaintools.com/content/iris-report-unc-1151-domains.pdf?utm_source=Blog&utm_campaign=IOC

[6] https://vsquare.org/the-ghostwriter-scenario/

Appendix (IOCs)

PACT Assesses with High Confidence that the following domains are part of UNC1151 operations; additionally, they do not appear in public reporting that has surfaced as part of PACT's analysis:

1. account-signin.online
2. bigmir-net.online
3. bigmir-net.site
4. com-firewall.site
5. com-verification.site
6. fr-login.website
7. i-ua.site
8. id-passport.online
9. interia-pl.online
10. interia-pl.space
11. interia.site
12. is-lt.online
13. is-lt.site
14. login-credentials.online
15. login-inbox.site
16. mail-i-ua.site
17. mail-validation.online
18. meta-ua.site
19. must-have-oboron.space
20. net-login.online
21. net-login.site
22. net-login.space
23. net-login.website
24. net-mail.space
25. net-validate.space
26. net-verification.site
27. net-verification.website
28. oborona-ua.site

29. passport-account.online
30. passport-yandex.online
31. passport-yandex.site
32. protect-sale.site
33. receller.space
34. sales-oboron.space
35. signin-credentials.online
36. signin-inbox.online
37. signin-inbox.site
38. uazashita.space
39. vilni-ludi.space
40. vp-pl.site
41. vp-pl.website
42. webmail-meta.online
43. wirtualna-polska.online
44. wp-dostep.website
45. wp-firewall.site
46. wp-pl.online
47. wp-pl.site
48. wp-pl.space
49. wp-pl.website
50. yahoo-com.site
51. yahoo-com.space
52. Zahist-ua.space

The following domains have been previously attributed as part of UNC1151 operations:

1. account-inbox.online
2. accounts-login.online
3. accounts-telekom.online
4. com-account.website
5. com-validate.site
6. com-verify.site
7. credentials-telekom.online
8. google-com.online
9. inbox-admin.site
10. interia-pl.site
11. interia-pl.website
12. login-inbox.online
13. login-mail.online
14. login-telekom.online
15. login-verify.online
16. logowanie-pl.site

17. meta-ua.online
18. mil-secure.site
19. net-account.online
20. net-account.space
21. net-support.site
22. net-verification.online
23. net-verify.site
24. onet-pl.online
25. op-pl.site
26. potwierdzenie.site
27. ron-mil-pl.site
28. ron-mil-pl.space
29. ru-mailbox.site
30. ru-passport.online
31. secure-firewall.online
32. secure-firewall.site
33. signin-telekom.online
34. ua-agreements.online
35. ua-login.site
36. ua-passport.online
37. ukroboronprom-com.site
38. ukroboronprom.online
39. verify-ua.online
40. verify-ua.site
41. verify-ua.space
42. wp-agreements.online
43. wp-pl-potwierdz-dostep.site
44. wp-pl.eu
45. wp-potwierdzac.site

PACT Assesses with Moderate Confidence that the following domains are part of phishing infrastructure that UNC1151 used; additionally, they do not appear in public reporting that has surfaced as part of PACT's analysis:

1. appie.in
2. apple-email.online
3. apple-emails.online
4. betlimanpark.com
5. com-direct.in
6. com-directly.in
7. com-id.info
8. com-id.site
9. com-idlog.in

10. com-idlogin.in
11. com-idlogin.site
12. com-ids.in
13. com-ids.info
14. com-idsign.in
15. com-idsite.in
16. com-last.info
17. com-latest.info
18. com-latestlocation.info
19. com-locations.info
20. com-logs.in
21. com-map.tech
22. com-site.id
23. com-site.in
24. com-sys.in
25. emails-apple.live
26. eu-icloud.com
27. europe-apple.com
28. europe-icloud.com
29. idlog.in

Matt Stafford, Senior Threat Intelligence Researcher